User Guide

hp StorageWorks Fabric OS 4.2.x Procedures

First Edition (April 2004)

Part Number: AA–RV2BA–TE

This document provides procedures for SAN administrators to set up and manage HP StorageWorks SANs. This document is specific to Fabric OS 4.2.x and the switches running Fabric OS 4.2.x.

Fabric OS 4.2.x Procedures User Guide
First Edition (April 2004)
Part Number: AA–RV2BA–TE

contents

Figures

Tables

about this guide

This document provides procedures for SAN administrators to set up and manage HP StorageWorks SANs. This document is specific to Fabric OS 4.2.x and the switches running Fabric OS 4.2.x.

This preface discusses the following major topics:

Audience

This book is intended for use by those responsible for monitoring and modifying their HP StorageWorks switch fabric.

Related Documentation

For the latest information, documentation, and firmware releases, visit the HP StorageWorks web site:
http://www.hp.com/country/us/eng/prodserv/storage.html.

To access the technical documentation:

1. Locate the **Networked storage** section of the Web page.
2. Under **Networked storage**, go to the **By type** subsection.
3. Click **SAN infrastructure**. The **SAN infrastructure** page opens.
4. Locate the **Fibre Channel Switches** section.
5. Click the appropriate product name. The product overview page opens. Go to the **product information** section.
6. Click **technical documents**.

For information about Fibre Channel standards, visit the Fibre Channel Industry Association web site, located at http://www.fibrechannel.org.

Conventions

Conventions consist of typographical elements and text symbols.

Typographical elements

This document follows the conventions in Table 1.

Table 1: Typography

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons; key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input and commands; code, file, and directory names; and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Getting help

If you have any questions associated with the information in this document, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP storage web site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP authorized reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, refer to the HP web site for locations and telephone numbers: http://www.hp.com.

Initial Configuration

1

This chapter discusses initial configuration tasks and addresses the following major topics:

Logging into the Switch

To log in to a switch using a Telnet connection:

1. Verify that the switch is connected to your IP network through the RJ-45 Ethernet port. At least one switch in the fabric must be connected through the Ethernet port in order to open a Telnet connection to the switch. For redundancy, HP recommends that at least two switches in your fabric be connected to your IP network.
2. Open a Telnet connection to the switch.

   The login prompt is displayed if the Telnet connection successfully found the switch in the network. If you log in to one logical switch, you are prompted to enter the logical switch number.
3. Enter the user ID (usually user or admin) at the login prompt.
4. Enter the password.

   If you are logging in for the first time, enter the default password: `password`. You are prompted to change the system passwords. You can press **CNTRL + C** to skip these prompts. You are prompted at each subsequent login until all the system passwords have been changed from the default values. You cannot use the `passwd` command until all account passwords have been changed from the default value, using the prompts at initial login.
5. Enter your new system passwords or press **CNTRL + C** to skip this prompt.
6. Verify that the login was successful. A prompt is displayed showing the switch name and user ID to which you are logged in. For example:

   ```
   login: admin
   password: xxxxxxx
   switch:admin>
   ```

Changing the System Passwords

As a security measure, the first time you log in to the Fabric OS, you are requested to change the system passwords. There are four account levels: root, factory, admin, and user. You cannot re-use the default passwords. Refer to the `passwd` command in the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for detailed information on the character limitations of passwords.

Note: Record these passwords exactly as entered, and save them in a secure location.

Note: HP recommends that you perform all switch configuration, management, and monitoring tasks from the admin or user account levels.

To change the system passwords at first login:

1. Log in to the switch as admin. The default password for the admin is `password`.
2. At first login you are prompted to change all the system passwords.
3. At the `Enter new password` prompt for the root account, enter a new root password.
4. At the `Enter new password` prompt for the factory account, enter a new factory password.
5. At the `Enter new password` prompt for the admin account, enter a new admin password.
6. At the `Enter new password` prompt for the user account, enter a new user password.

7. Record these passwords exactly as entered, and save them in a secure location. For example:

```
Fabric OS (cp0)

cp0 login: admin
Password:
Please change your passwords now.
Use Control-C to exit or press 'Enter' key to proceed.

for user - root
Changing password for root
Enter new password:
Password changed.
Saving password to stable storage.
Password saved to stable storage successfully.

Please change your passwords now.
for user - factory
Changing password for factory
Enter new password:
Password changed.
Saving password to stable storage.
Password saved to stable storage successfully.

Please change your passwords now.
for user - admin
Changing password for admin
Enter new password:
Password changed.
Saving password to stable storage.
Password saved to stable storage successfully.

Please change your passwords now.
```

```
for user - user
Changing password for user
Enter new password:
Password changed.
Saving password to stable storage.
Password saved to stable storage successfully.
switch:admin>
```

Connecting through the Serial Interface

There are a few procedures that require you connect through the serial port; for example, setting the boot PROM and recovery passwords.

Use this procedure when connecting to the serial port.

1. Connect the serial cable to the serial port on the switch, and to an RS-232 serial port on the workstation.

   If the serial port on the workstation is RJ-45 instead of RS-232, remove the adapter on the end of the serial cable and insert the exposed RJ-45 connector into the RJ-45 serial port on the workstation.

2. Disable any serial communication programs running on the workstation.
3. Open a terminal emulator application (such as HyperTerminal on a PC, or TERM or Kermit in a UNIX® environment), and configure the application as follows:
   — In a Windows® 95, 98, 2000, or Windows NT® environment:

     Parameter: Value

     Bits per second: 9600

     Databits: 8

     Parity: None

     Stop bits: 1

     Flow control: None

   — In a UNIX environment, enter the following string at the prompt:

     ```
     tip /dev/ttyb -9600
     ```

Setting the Boot PROM and Recovery Passwords

The Boot PROM and Recovery passwords provide an additional layer of security beyond the root password.

- Setting a Boot PROM password protects the boot prompt from unauthorized use.
- Setting a Recovery password turns on the password recovery option, which requires a user to contact Technical Support before recovering a root or boot PROM password.

Note: HP strongly recommends setting both the Boot PROM and Recovery passwords on all switches running Fabric OS v4.2.x. Not setting either of these passwords can compromise fabric security.

- To set the Boot PROM password without setting the Recovery password, see "Setting the Boot PROM Password Only (SAN Switch 2/32)" on page 111.
- To set the Boot PROM password and Recovery password, follow these steps:

Note: Some steps are specific to the HP StorageWorks Core Switch 2/64 and HP StorageWorks SAN Director 2/128. These steps are preceded by *(2/64 and 2/128 only)*.

---

1. (2/64 and 2/128 only) Determine the active CP card by opening a Telnet session to either CP card, logging in as admin, and entering the `hashow` command.
2. Create a serial connection to the switch. (See "Connecting through the Serial Interface" on page 35.)
3. (2/64 and 2/128 only) Log in to the active CP card by serial or Telnet and enter the `hadisable` command to prevent failover during the remaining steps.

4. Follow the directions below for your particular switch:
   - (2/64 only) Reboot the standby CP card by pressing the yellow ejector buttons at top and bottom of the CP card, then pressing both ejector handles back towards the switch to lock the card back into the slot.
   - (2/128 only) Reboot the standby CP card by sliding the On/Off switch on the ejector handle of the standby CP card to Off, and then back to On.
   - (All other switches) Reboot.
5. Press **ESC** within four seconds after the message `Press escape within 4 seconds.` displays.

   The following options are available:
   - Start system.
   - Recovery password.
   - Enter command shell.
6. Enter `2` at the prompt to set the Recovery password. The message `Recovery password is NOT set. Please set it now.` displays.
7. Enter the Recovery password. The Recovery password must be between 8 and 40 alphanumeric characters. For higher security, HP recommends a random password that is 15 characters or longer. The firmware prompts only this password only once. It is not necessary to record the Recovery password.

   The prompt `New password` displays.

Note: It is extremely important that you note and safely store the boot PROM password. The password may be required to troubleshoot a switch, so having the password available can save valuable time. Recovering the password is a time-consuming process, and requires contacting Technical Support.

---

8. Enter the Boot PROM password, then reenter when prompted. Record this password for future use.

   The new passwords are automatically saved (the `saveenv` command is not required).

9. Follow step b for a switch other than a Core Switch 2/64 or a SAN Director 2/128; for a Core Switch 2/64 or a SAN Director 2/128, follow step a.
   a. (2/64 and 2/128 only) Fail over the active CP card by entering the `hafailover` command. Traffic flow through the active CP card resumes when the failover is complete.
   b. (All other switches) Reboot. Traffic flow resumes when the switch finishes rebooting.

      This completes the steps for a switch other than Core Switch 2/64 and SAN Director 2/128.
10. (2/64 and 2/128 only) Connect the serial cable to the serial port on the new standby CP card (previous active CP card).
11. (2/64 and 2/128 only) Repeat step 3 through step 8 for the new standby CP card (each CP card has a separate Boot PROM password).
12. (2/64 and 2/128 only) Log in to the active CP card by serial or Telnet and enter the `haenable` command to restore high availability.

Configuring the Switch Names

You can customize the switch names for the logical switches. If you chose to change the default switch name, use a switch name that is unique and meaningful.

Note: Changing a switch name causes a domain address format RSCN to be issued.

Switch Names

- Can be up to 15-characters long for v4.2.x

Note: This is shorter than under v3.x, which allows names up to 19 characters.

- Must begin with an alpha character
- Can consist of any combination of alphanumeric and underscore characters

(For Core Switch 2/64 only) The default names are “sw0” for the switch containing the port cards in slots 1-4, and “sw1” for the switch containing port cards in slots 7-10.

To customize the switch name:

1. Verify the CP to which the serial cable is connected.
2. Log in to the switch as admin.
3. (For Core Switch 2/64 only) Choose the logical switch that you want to change. Enter the value that corresponds to that logical region:
   — Enter `0` to configure logical switch 0 (slot 1 through 4)
   — Enter `1` to configure logical switch 1 (slot 7 through 10)
4. Enter the `switchname` command.
5. Enter the new name in quotes, as shown in the following example:

   ```
   switchname "sw10"
   ```

   For more information about this command, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.
6. Record the new switch name for future reference.
7. (Optional) Log out of the CP session, and repeat step 1 through step 6 for the second logical switch.

Managing Licensed Features

Licensed features such as Zoning, Performance Monitor, and Web Tools are already loaded onto the switch firmware, but must be enabled with a license key. After you have purchased these features, you are provided with a key to enable the features; see "Obtaining Optional Software License Keys from HP" on page 40.

You can use several access methods to manage the switch (after the IP addresses are set), including:

- Fabric OS CLI (Telnet)
- Web Tools
- Fabric Manager
- A third party application using the API

Obtaining Optional Software License Keys from HP

If you have purchased optional software, or need to reinstall software features due to a motherboard replacement in your switch, you will need to retrieve the software license keys from the HP Authorization Center.

Obtain software license keys as follows:

- If you have your HP Registration Number (located on your software entitlement certificate), go to http://webkey.external.hp.com/welcome.asp.
- If your HP Registration Number is unavailable, contact the Authorization Center directly:
  - Canada and United States, Monday through Friday 6:00 am to 6:00 pm MST, (801) 431-1451 or (800) 861-2979.
  - Asia, Monday through Friday 9:00 am to 5:00 pm, +81-03-3227-5289 or +81-3-3227-5289.
  - Europe, Middle East, Africa and Netherlands, Monday through Friday 9:00 am to 6:00 pm, +31-555-384-210.

Activating a License

Follow these steps to activate a license on a switch using the command line interface:

1. Log in to the switch as admin.
2. To activate a license, you must have a valid license key. Use the license key provided in the licensed Paper Pack supplied with switch software, or follow the procedure in section "Obtaining Optional Software License Keys from HP" on page 40 to generate a license key.

   Activate the license using the `licenseadd` command, as follows:

   ```
   switch:admin> licenseadd "key"
   ```

Note: The license key is case sensitive and must be entered exactly as given. The double quotes are optional.

---

3. Verify the license was added by issuing the `licenseshow` command.

A list displays all of the licenses currently installed on the switch. For example:

```
switch:admin> licenseshow
AbbbcDefcQxdezdr:
    Web license
    Zoning license
    SES license
    Fabric license
    Remote Switch license
    Extended Fabric license
    Entry Fabric license
    Fabric Watch license
    Performance Monitor license
    Trunking license
    Security license
switch:admin>
```

If the licensed feature is listed, the feature is installed and immediately available. If the license is not listed, repeat step 2 of this procedure.

Verifying License Activation

To verify that all required licenses are activated on the switch, perform the following steps:

1. Log in to the switch as admin.
2. Enter the `licenseshow` command.

A list displays all of the licenses currently activated on the switch. For example:

```
switch:admin> licenseshow
AbbbcDefcQxdezdr:
    Web license
    Zoning license
    Fabric license
    Remote Switch license
    Remote Fabric license
    Extended Fabric license
    Entry Fabric license
    Fabric Watch license
    Performance Monitor license
    Trunking license
    Security license
switch:admin>
```

If the licensed feature is listed, the feature is installed and immediately available. If the license is not listed, follow the procedure in "Activating a License" on page 40 to activate the license.

Note: To activate a license, you need a valid license key. See "Obtaining Optional Software License Keys from HP" on page 40 for instructions on generating single or multiple license keys.

Configuring Fabric Parameters

Fabric parameters include all the items listed in the `configure` command. They can be displayed with the `configshow` command, and must be identical for each switch across a fabric.

To save time when configuring the fabric parameters:

Caution: PID addressing format is an option of the `configure` command. The default under v4.x is Core PID, also called Switch Format 1; this is not the default on Fabric OS 2.x and Fabric OS 3.x.

If you are adding a Fabric 4.x switch to a fabric with other earlier firmware level switches you need to decide on a Switch PID format. Mixed PID formats in a fabric result in fabric segmentation. For detailed information regarding PID formats and related procedures, see Chapter 13, "Initial Configuration."

1. Configure one switch first (using the `configure` command)
2. Use the `configUpload` command to save the configuration information. See "Saving the Switch Configuration File to a Host" on page 50.
3. Use the `configdownload` command to download the configuration information onto each of the remaining switches. See "Restoring the Fabric Configuration Settings" on page 68.

Setting Additional Fabric Configurations

In addition to the configuration parameters set through the `configure` command, additional parameters can be set.

Some additional configuration options to consider include:

- Set Routing - see "Routing" on page 79.
- Track Changes - see "Tracking Switch Changes" on page 77.
- Status Policies - see "Switch Status Policies" on page 73.

Configuring Software Features

You must configure software features (such as Fabric Watch, Zoning, and Secure Fabric OS) for the fabric.

To save time, configure the software features on one switch, then save the configuration file, and download it to the each of the remaining switches. See "Saving the Switch Configuration File to a Host" on page 50; HP recommends that you download configuration files only to switches of the same switch type.

Verifying Switch Operation

To verify that your switch is operating correctly, display switch and port status, and assess the status output for correct switch operation:

1. Log in to the switch as admin.
2. Enter the `switchshow` command. This command displays a switch summary and a port summary.

   The following example displays the `switchshow` command on a Core Switch 2/64:

```
switch:admin> switchshow
switchName: switch
switchType:     10.1
switchState:    Online
switchRole:     Subordinate
switchDomain:   1
switchId:       fffc01
switchWwn:      10:00:00:60:69:80:04:5a
switchBeacon:   OFF
blade1 Beacon:  OFF
blade3 Beacon:  OFF

Area Slot Port Gbic Speed State
=====================================
0    1    0   id    N2   No_Light
1    1    1   id    N2   No_Light
2    1    2   --    N2   No_Module
3    1    3   id    N2   Online    E-Port 10:00:00:60:69:80:04:5b
"ulys62" (Trunk master)
4    1    4   id    N2   No_Light
5    1    5   id    N2   Online    E-Port 10:00:00:60:69:00:54:e9
"san78" (upstream)(Trunk master)
6    1    6   id    N2   No_Light
7    1    7   id    N2   No_Light
8    1    8   --    N2   No_Module
9    1    9   id    N2   No_Light
10    1   10   id    N2   Online    E-Port10:00:00:60:69:90:02:5e
"sqad120" (downstream)(Trunk master)
11    1   11   --    N2   No_Module
12    1   12   id    N2   No_Light
13    1   13   --    N2   No_Module
14    1   14   id    N1   Online    F-Port21:00:00:e0:8b:03:70:b1
. . . .
(Continued)
15    1   15   id    N2   Online    E-Port
10:00:00:60:69:90:02:5e "sqad120" (Trunk master)

32    3    0   id    N2   No_Light
33    3    1   --    N2   No_Module
34    3    2   id    N2   Online    Loopback->Slot  3 Port  2
35    3    3   id    N2   No_Light
```

```
36    3    4   id    N2   No_Light
37    3    5   id    N2   Online    E-Port
10:00:00:60:69:00:54:ea "san79" (Trunk master)
38    3    6   id    N2   No_Light
39    3    7   id    N2   No_Light
40    3    8   id    N2   Online    E-Port  (Trunk port, master
is Slot  3 Port 9)
41    3    9   id    N2   Online    E-Port
10:00:00:60:69:80:04:5b "ulys62" (Trunk master)
42    3   10   id    N2   Online    E-Port  (Trunk port, master
is Slot  3 Port 9)
43    3   11   id    N2   Online    E-Port  (Trunk port, master
is Slot  3 Port 9)
44    3   12   id    N2   No_Light
45    3   13   id    N2   No_Light
46    3   14   id    N2   No_Light
47    3   15   id    N1   Online    L-Port  2 public
switch:admin>
```

3. Check that the switch and ports are online.

Verifying Hi-Availability (HA)

1. Log in to the switch as admin.
2. Enter the `hashow` command.

   Verify that HA is enabled, that the heartbeat is up, and that the HA state is in sync. For example:

   ```
   switch:admin> hashow

   Local CP (Slot 5, CP0): Active

   Remote CP (Slot 6, CP1): Standby, Healthy

   HA enabled, Heartbeat Up, HA State synchronized
   ```

3. (Optional) Enter the `chassisshow` command to verify operation of the Field Replaceable Units (FRUs). For example:

   ```
   switch12k:admin> chassisshow

   SW BLADE Slot: 3
   Header Version: 1
   Power Consume Factor: -180
   HP Part Num: 60-0001532-03
   HP Serial Num: 1013456800
   Manufacture: Day: 12 Month: 6 Year: 2001
   Update: Day: 15 Month: 7 Year: 2001
   Time Alive: 28 days
   Time Awake: 16 days
   ID: 555-374757q> to stop
   ```

```
Part Num: 234-294-12345
Serial Num: 2734658
Revision Num: A.00

CP BLADE Slot: 6
Header Version: 1
Power Consume Factor: -40
HP Part Num: 60-0001604-02
HP Serial Num: FP00X600128
Manufacture: Day: 12 Month: 6 Year: 2001
Update: Day: 15 Month: 7 Year: 2001
Time Alive: 61 days
Time Awake: 16 days
ID: 555-374757
Part Num: 236-296-12350
Serial Num: 2836542
Revision Num: A.00

POWER SUPPLY Unit: 2
Header Version: 1
Power Consume Factor: 1000
HP Part Num: 60-0001536-02to stop
HP Serial Num: A013450700
Manufacture: Day: 14 Month: 6 Year: 2001
Update: Day: 15 Month: 7 Year: 2001
Time Alive: 50 days
Time Awake: 16 days
ID: 555-374757
Part Num: 238-298-12360
Serial Num: 1234567

<output truncated>
```

4. (Optional) Enter the `slotshow` command to inventory and display the current status of each slot in the system. For example:

```
switch:admin> slotshow

Slot Blade Type ID Status

---------------------------------

1 SW BLADE 2 FAULTY

2 SW BLADE 2 DISABLED

3 SW BLADE 2 ENABLED

4 SW BLADE 2 DIAG RUNNING POST2

5 CP BLADE 1 ENABLED

6 CP BLADE 1 ENABLED

7 UNKNOWN VACANT

8 SW BLADE 2 DIAG RUNNING POST1

9 SW BLADE 2 INSERTED, NOT POWERED ON

10 UNKNOWN VACANT
```

Verifying the Fabric Connectivity

To view and verify all switches in a fabric, display a summary of information about the fabric.

1. Log in to the switch as admin.
2. Enter the `fabricshow` command. This command displays a summary of all the switches in the fabric. For example:

```
switch:admin> fabricshow
Switch ID   Worldwide Name           Enet IP Addr    FC IP Addr      Name
-------------------------------------------------------------------------
  1: fffc01 10:00:00:60:69:80:04:5a  192.168.186.61  192.168.68.193  "switch61"
  3: fffc03 10:00:00:60:69:10:9c:29  192.168.186.175 0.0.0.0         "switch175"
  4: fffc04 10:00:00:60:69:12:14:b7  192.168.174.70  0.0.0.0         "switch70"
  5: fffc05 10:00:00:60:69:45:68:04  192.168.144.121 0.0.0.0         "switch121"
  6: fffc06 10:00:00:60:69:00:54:ea  192.168.174.79  192.168.68.197  "switch79"
  7: fffc07 10:00:00:60:69:80:04:5b  192.168.186.62  192.168.68.194  "switch62"
  8: fffc08 10:00:00:60:69:04:11:22  192.168.186.195 0.0.0.0        >"switch195"
  9: fffc09 10:00:00:60:69:10:92:04  192.168.189.197 192.168.68.198  "switch197"
 10: fffc0a 10:00:00:60:69:50:05:47  192.168.189.181 192.168.68.181  "switch181"
 11: fffc0b 10:00:00:60:69:00:54:e9  192.168.174.78  192.168.68.196  "switch78"
 15: fffc0f 10:00:00:60:69:30:1e:16  192.168.174.73  0.0.0.0         "switch73"
 33: fffc21 10:00:00:60:69:90:02:5e  192.168.144.120 0.0.0.0         "switch120"
 44: fffc2c 10:00:00:60:69:c0:06:8d  192.168.144.121 0.0.0.0         "switch121"
```

```
 97: fffc61 10:00:00:60:69:90:02:ed  192.168.144.123 0.0.0.0         "switch123"
 98: fffc62 10:00:00:60:69:90:03:32  192.168.144.122 0.0.0.0         "switch122"

The Fabric has 15 switches

switch:admin>
```

Connecting Devices to the Switch

Power off all devices (to minimize port logins [PLOGIs]) and connect them to the switch, according to your topology. For devices that cannot be powered off, connect the devices, but use the `portdisable` command to disable the port on the switch.

When powering the devices back on, wait for each device to complete the fabric login before powering on the next one.

Verifying Device Connectivity

To view and verify that you have fabric-wide device connectivity, display the fabric-wide device count. The number of devices listed in the Name Server (NS) should reflect the number of devices that are connected.

1. Log in to the switch as admin.
2. (Optional) Enter the `switchshow` command to verify that the storage devices are logged in.
3. (Optional) Enter the `nsshow` command to verify that the storage devices have successfully registered with the Name Server.

4. Enter the `nsallshow` command. This command displays 24-bit Fibre Channel addresses of all devices in the fabric. For example:

```
switch:admin> nsallshow
75 Nx_Ports in the Fabric {
  010e00 012fe8 012fef 030500 030b04 030b08 030b17 030b18
  030b1e 030b1f 040000 050000 050200 050700 050800 050de8
  050def 051700 061c00 071a00 073c00 090d00 0a0200 0a07ca
  0a07cb 0a07cc 0a07cd 0a07ce 0a07d1 0a07d2 0a07d3 0a07d4
  0a07d5 0a07d6 0a07d9 0a07da 0a07dc 0a07e0 0a07e1 0a0f01
  0a0f02 0a0f0f 0a0f10 0a0f1b 0a0f1d 0b2700 0b2e00 0b2fe8
  0b2fef 0f0000 0f0226 0f0233 0f02e4 0f02e8 0f02ef 210e00
  211700 211fe8 211fef 2c0000 2c0300 611000 6114e8 6114ef
  611600 620800 621026 621036 6210e4 6210e8 6210ef 621400
  621500 621700 621a00
}
switch:admin>
```

Backing Up Switch Configuration Information

You should make both a hard copy backup of switch information and save a copy of the switch configuration file to a host.

Making a Hard Copy of Switch Information

HP recommends that you make a hard copy backup of all key configuration data, including license key information for every switch, and store it in a safe and secure place for emergency reference. See the following procedures.

1. Print out the information from the following command and store in a secure location:

   `licenseshow` - Displays the license keys you have installed.

2. Print out the information from the following command and store in a secure location:

   `configshow` - Displays configuration parameters and setup information. Refer the discussion of the `configshow` command in the *HP StorageWorks Fabric OS 4.2.x User Guide* for more information.

3. Print out the information from the following command and store in a secure location:

   ```
   ipaddrshow
   ```

Note: Depending on the security procedures of your company, you may want to keep a record of the user levels and passwords for all switches in the fabric. This is sensitive information; access to such information should be limited.

Saving the Switch Configuration File to a Host

HP recommends that you save all key configuration data, including license key information for every switch and upload it to a host for emergency reference.

About the Configuration File

The configuration file is written as three sections, and is broken up as follows:

- The first section contains the switch boot parameters. It has variables such as the switch's name and IP address. This section corresponds to the first few lines of output of the `configshow` command.
- The second section contains general switch configuration variables, such as diagnostic settings, fabric configuration settings, and SNMP settings. This section corresponds to the output of the `configshow` command (after the first few lines), although there are more lines uploaded than are shown by the command.
- The third section contains zoning configuration parameters.

To save a backup copy of the configuration file to a host:

1. Verify that the FTP service is running on the host workstation (or on a Windows machine).
2. Log in to the switch as the admin.

3. Enter the `configupload` command, as discussed below.
   - Enter the command only, then enter the options as you are prompted; or enter:
   - `configupload ["host","user","file"[,"passwd"]]`

     where the parameters are as follows:

host	Optional operand that specifies a host name or IP address in quotation marks; for example, "`citadel`" or "`192.168.1.48`". The configuration file is downloaded from this host system.
user	Optional operand that specifies a user name in quotation marks; for example, "`jdoe`". This user name is used to gain access to the host.
file	Optional operand that specifies a file name in quotation marks; for example, "config.txt". Absolute path names may be specified using the forward slash (/). Relative path names create the file in the user's home directory on UNIX hosts, and in the directory where the FTP server is running on a Windows hosts.
passwd	Optional operand that specifies a password in quotation marks.

For example:

```
switch:admin> configupload "citadel", "jdoe", "config.txt",
"passwd"

upload complete

switch:admin>
```

A message is displayed that the upload is complete.

Basic Switch Management

2

This chapter provides information on basic management tasks for a switch.

The following procedures are described in this chapter:

Switch Enable and Disable Procedures

This section includes the following procedures:

- "Enabling a Switch" on page 54
- "Disabling a Switch" on page 54
- "Enabling a Port" on page 54
- "Disabling a Port" on page 57

Enabling a Switch

To enable a switch:

1. Log in to the switch as admin.
2. Issue the `switchenable` command.

   All Fibre Channel ports that passed the POST test are enabled. If the switch was part of a fabric, it rejoins the fabric. For example:

```
switch:admin> switchenable
10 9 8 7 6 5 4 3 2 1
fabric: Principal switch
fabric: Domain 1
switch:admin>
```

Disabling a Switch

To disable a switch:

1. Log in to the switch as the admin.
2. Issue the `switchdisable` command.

   All fibre channel ports on the switch are taken offline, if the switch was part of a fabric, the fabric reconfigures. For example:

```
switch:admin> switchdisable
```

Enabling a Port

To enable a port:

1. Log in to the switch as admin.
2. Issue the `portenable` command, using the following syntax:

Specify the *slotnumber* and *portnumber,* separated by a slash, as the slot and port number of the port you want to enable. If the port is connected to another switch, the fabric may reconfigure. If the port is connected to one or more devices, these devices become available to the fabric.

The following example is the `portenable` command output from an HP StorageWorks Core Switch 2/64.

```
switch:admin> portenable 3/7
switch:admin> portshow 3/7
portName:
portDisableReason: None
portCFlags: 0x1 ENABLED
portFlags: 0x20041       PRESENT U_PORT LED
portType: 4.2.x
portState: 2    Offline
portPhys: 4    No_Light
portScn:   0
portId:    012700
portWwn:   20:27:00:60:69:80:04:5a
portWwn of device(s) connected:
        None
Distance: normal
Speed: N2Gbps

Interrupts:       3        Link_failure: 0        Frjt:
0
Unknown:          0        Loss_of_sync: 0        Fbsy:
0
Lli:               3          Loss_of_sig: 3
Proc_rqrd:         0          Protocol_err: 0
Timed_out:         0          Invalid_word: 0
Rx_flushed:        0          Invalid_crc: 0
Tx_unavail:        0          Delim_err:    0
Free_buffer:       0          Address_err: 0
Overrun:           0          Lr_in:        0
Suspended:         0          Lr_out:       0
```

```
Parity_err:         0           Ols_in:       0
2_parity_err:       0           Ols_out:      0
CMI_bus_err:        0
switch:admin>
```

The following example shows `portenable` command output from an HP StorageWorks SAN Switch 2/32.

```
switch:admin> portenable 4
switch:admin> portshow 4
portName:
portDisableReason: None
portCFlags: 0x1
portFlags: 0x20041       PRESENT U_PORT LED
portType: 4.2.x
portState: 2    Offline
portPhys: 4    No_Light
portScn:   0
portId:    010400
portWwn:   20:04:00:60:69:90:03:56
portWwn of device(s) connected:
        None
Distance: normal
Speed: N2Gbps

Interrupts:       363       Link_failure: 8         Frjt:
0
Unknown:          0         Loss_of_sync: 0         Fbsy:
0
Lli:                23         Loss_of_sig: 3
Proc_rqrd:          340        Protocol_err: 0
Timed_out:          0          Invalid_word: 0
Rx_flushed:         0          Invalid_crc: 0
Tx_unavail:         0          Delim_err:    0
Free_buffer:        0          Address_err:  0
```

```
Overrun:            0          Lr_in:        4
Suspended:          0          Lr_out:       4
Parity_err:         0          Ols_in:       4
2_parity_err:       0          Ols_out:      4
CMI_bus_err:        0
switch:admin>
```

Disabling a Port

To disable a port:

1. Log in to the switch as admin.
2. Issue the `portdisable` command:

   `portdisable [slotnumber]/portnumber`

Note: Slot number is required only for the Core Switch 2/64 switch.

(Optional) Specify the *slotnumber* and *portnumber* that you want to disable. If the port is connected to another switch, the fabric may reconfigure. If the port is connected to one or more devices, these devices are no longer available to the fabric.

The following examples show how to disable a port for a Core Switch 2/64 and a SAN Switch 2/32.

This example is for a Core Switch 2/64.

```
switch:admin> portdisable 1/2
switch:admin> portshow 1/2
portName:
portHealth: OFFLINE
portDisableReason: None
portCFlags: 0x0
portFlags: 0x4021        PRESENT U_PORT DISABLED LED
portType:  4.2
portState: 2    Offline
portPhys:  6    In_Sync
portScn:   2    Offline
```

```
portId:    0a0200
portWwn:   20:02:00:60:69:80:4f:84
portWwn of device(s) connected:
        None
Distance:  normal
portSpeed: N2Gbps

Interrupts:       1356      Link_failure: 2         Frjt:
0
Unknown:          4         Loss_of_sync: 0         Fbsy:
0
Lli:              9         Loss_of_sig:   0
Proc_rqrd:        1343      Protocol_err: 0
Timed_out:        0         Invalid_word: 0
Rx_flushed:       0         Invalid_crc:   0
Tx_unavail:       0         Delim_err:     0
Free_buffer:      0         Address_err:   0
Overrun:          0         Lr_in:         1
Suspended:        0         Lr_out:        1
Parity_err:       0         Ols_in:        1
2_parity_err:     0         Ols_out:       0
CMI_bus_err:      0

switch:admin> portenable 1/2
switch:admin>
```

This example is for a SAN Switch 2/32.

```
switch:admin> portdisable 4
switch:admin> portshow 4
portName:
portDisableReason: None
portCFlags: 0x1
portType:  4.2.x
portState: 2    Offline
portPhys:  4    No_Light
```

```
portScn:    0
portId:     010400
portWwn:    20:04:00:60:69:90:03:56
portWwn of device(s) connected:
        None
Distance:  normal
Speed: N2Gbps

Interrupts:       362       Link_failure: 8         Frjt:
0
Unknown:          0         Loss_of_sync: 0         Fbsy:
0
Lli:                22         Loss_of_sig:   2
Proc_rqrd:          340        Protocol_err:  0
Timed_out:          0          Invalid_word:  0
Rx_flushed:         0          Invalid_crc:   0
Tx_unavail:         0          Delim_err:     0
Free_buffer:        0          Address_err:   0
Overrun:            0          Lr_in:         4
Suspended:          0          Lr_out:        4
Parity_err:         0          Ols_in:        4
2_parity_err:       0          Ols_out:       4
CMI_bus_err:        0
switch:admin>
```

Domain IDs

Domain IDs are assigned dynamically when a switch is enabled. The Domain ID can be set manually, however, to control the number or to resolve a Domain ID conflict when merging fabrics.

Displaying a Current List of Domain IDs

1. Log in to a switch.
2. Issue the `fabricshow` command.

Fabric information is displayed, including the Domain ID (D_ID). For example:

```
switch:admin> fabricshow
Switch ID Worldwide Name Enet IP Addr FC IP Addr Name
-------------------------------------------------------------------
3: fffc43 10:00:00:60:69:10:60:1f 192.168.64.187 0.0.0.0 "sw187"
2: fffc42 10:00:00:60:69:00:05:91 192.168.64.60 192.168.65.60 "sw60"
1: fffc41 10:00:00:60:69:00:02:0b 192.168.64.180 192.168.65.180>"sw180"
0: fffc40 10:00:00:60:69:00:06:56 192.168.64.59 192.168.65.59 "sw5"
The Fabric has 4 switches
Group ID Token
-----------------
0: fffb01 40:05:00:00:10:00:00:60:69:00:00:15
```

The fields in the `fabricshow` command are described as follows:

- Switch ID: the switch Domain_ID and embedded port D_ID
- Worldwide Name: the switch WWN
- Enet IP Addr: the switch Ethernet IP address
- FC IP Addr: the switch FC IP address
- Name: the switch symbolic name. An arrow (>) indicates the principal switch

If multicast alias groups exist, the following fields are shown:

- Group ID: the alias group number and D_ID
- Token: the alias group token (assigned by the N_Port)

Setting a Domain ID

For the Core Switch 2/64, the default domain ID for both logical switches is 1. To prevent a domain ID conflict, you can either make the domain IDs unique before connecting the logical switches to the fabric, or disable one of the switches until both are connected to the fabric, then reenable (unique domain IDs are automatically assigned).

1. Log in to the switch.
2. Issue the `switchdisable` command to disable the switch.
3. Issue the `configure` command.
4. Enter `Y` after the `Fabric parameters` prompt. For example:

```
Fabric parameters (yes, y, no, n): [no] y
```

5. Enter a unique domain ID at the domain ID prompt. For example:

```
Domain: (1..239) [1] 3
```

6. Complete the remaining prompts (or press **CTRL+D** to accept the other settings and exit).
7. Issue the `switchenable` command to reenable the switch.

Firmware Versions

For information regarding performing firmware downloads, see Chapter 4, "Downloading Firmware."

Different HP StorageWorks switches run on different versions of Fabric OS firmware. Table 2 describes the switch type and the corresponding firmware.

Table 2: Switch Type and Correct Firmware

Switch Type	Correct Firmware
1 GB	Fabric OS 2.x
SAN Switch 2/8-EL, SAN Switch 2/16-EL, and SAN Switch 2/16	Fabric OS 3.x
SAN Switch 2/32	Fabric OS 4.0.2x or later.
Core Switch 2/64	Fabric OS 4.x
SAN Director 2/128	Fabric OS 4.2.x or later

Note: If a SAN Switch 2/32 is running v4.2.x firmware (or later), HP recommends that all directly connected switches be running v2.6.2, v3.1.2, or v4.2.x before a subsequent firmware download is performed on the SAN Switch 2/32. See the Firmware Download section "Upgrading Firmware on the SAN Switch 2/32" on page 120 on for more detailed information.

Displaying the Firmware Version and Information

Use the `version` command to display firmware information and build dates.

To display the firmware version:

1. Log in to the switch as admin.
2. Issue the `version` command.

   This command displays the Kernel version, Fabric OS release number, and other information about the firmware.

The following example shows the firmware version information on a Core Switch 2/64. For example:

```
switch:admin> version
Kernel:     2.4.19
Fabric OS:  v4.2.x
Made on:    Tue Jun 24 09:36:37 2003
Flash:      Tue Jun 24 13:42:40 2003
BootProm:   3.2.4
switch:admin>
```

The following information is displayed in the `version` command:

Kernel:	Displays the version of switch kernel operating system
Fabric OS:	Displays the version of switch Fabric OS
Made on:	Displays the build date of firmware running in switch
Flash:	Displays the build date of firmware stored in flash proms
BootProm:	Displays the version of the firmware stored in the boot PROM

Usually the `Made on` and `Flash` dates are the same, since the switch starts running flash firmware at power-on. However, in the time between a `firmwareDownload` command and the next reboot, the dates can differ.

3. Issue the `firmwareShow` command.

   Use this command to display the Fabric OS versions on primary and secondary partitions on the local CP and on the remote CP. This command identifies the status for each CP as Active or Standby, and also identifies the slot number for each CP.

If there is only one CP available, the command displays the Fabric OS versions for the primary and secondary partitions on that CP. For example, for a SAN Switch 2/32:

```
switch2/32:admin> firmwareshow
Primary partition: v4.2.x
Secondary Partition: v4.2.x
switch2/32:admin>
```

Core Switch 2/64 example:

```
switch12k:admin> firmwareshow
Local CP (Slot 5, CP0): Active
        Primary partition:      v4.2.x
        Secondary Partition:    v4.2.x
Remote CP (Slot 6, CP1): Standby
        Primary partition:      v4.2.x
        Secondary Partition:    v4.2.x

Note: If Local CP and Remote CP have different versions
of firmware, please retry firmwaredownload command.
switch12k:admin>
```

Switch Date and Time

All switches maintain the current date and time in non-volatile memory. Date and time are used for logging events. Switch operation does not depend on the date and time; a switch with an incorrect date and time value still functions properly.

You can synchronize the local time of the Principal or Primary Fabric Configuration Server (FCS) switch to an external NTP server.

Note: The `date` and `tsclockserver` commands are disabled when the security feature is enabled. With security enabled, you can view only the current date setting, unless the commands are performed on the Primary FCS switch.

Setting the Switch Date and Time

To set the date and time of a switch:

1. Log in to the switch as the admin.
2. Issue the `date` command:

   ```
   date "MMDDhhmmYY"
   ```

   The values represent the following:

   — MM is the month, valid values are 01-12.

   — DD is the date, valid values are 01-31.

   — hh is the hour, valid values are 00-23.

   — mm is minutes, valid values are 00-59.

   — YY is the year, valid values are 00-99.

Note: Year values greater than 69 are interpreted as 1970-1999, year values less than 70 are interpreted as 2000-2069. The date function does not support daylight savings time or time zones, so changes have to be reset manually.

For example:

```
switch:admin> date
Fri May  5 21:50:00 UTC 1989
switch:admin>
switch:admin> date "0624165203"
Tue Jun 24 16:52:30 UTC 2003
switch:admin>
```

Synchronizing Local Time with an External Source

Use this procedure to synchronize the local time of the Principal or Primary FCS switch to an external NTP server.

1. Log in as admin.
2. Issue the `tsclockserver [`*`ipaddr`*`]` command

where *ipaddr* is the IP address of the NTP server. The *ipaddr* specified should be the IP address of an NTP server and should be accessible from the switch. This operand is optional; by default this value is `LOCL`. For example:

```
switch:admin> tsclockserver
LOCL
switch:admin> tsclockserver "132.163.135.131"
switch:admin> tsclockserver
132.163.135.131
switch:admin>
```

Correcting the Time Zone of a Switch

If the time of your switches is off by hours (and not minutes), use the following procedure on all switches to set the Time Zone.

1. Log in as admin.
2. Issue the `tstimezone` command as follows:

   `tstimezone` [*houroffset* [, *minuteoffset*]]

   For example:

   — For Pacific Standard Time enter `tsTimeZone -8,0`

   — For Central Standard Time enter `tsTimeZone -6,0`

   — For Eastern Standard Time enter `tsTimeZone -5,0`

   The default time zone for switches is Universal Time Conversion (UTC), which is 8 hours ahead of Pacific Standard Time. For additional time zone conversions, see "Direct Conversions from UTC to Local Time" on page 66.

   The parameters listed above would not apply if the time zone of the switches has already been changed from the default (8 hours ahead of PT).

   Refer to the `tstimezone` command in the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more detailed information about the command parameters.
3. Repeat step 1 and step 2 on all switches for which the time zone needs to be set. The time zone needs to be set only once since the value is written to flash.

Direct Conversions from UTC to Local Time

For US time zones, use the following information to determine the correct parameter for the `tstimezone` command:

Local Time	`tstimezone` parameter (difference from UTC)
Atlantic Standard	`-4,0`
Atlantic Daylight	`-3,0`
Eastern Standard	`-5,0`
Eastern Daylight	`-4,0`
Central Standard	`-6,0`
Central Daylight	`-5,0`
Mountain Standard	`-7,0`
Mountain Daylight	`-6,0`
Pacific Standard	`-8,0`
Pacific Daylight	`–7,0`
Alaskan Standard	`-9,0`
Alaskan Daylight	`-8,0`
Hawaiian Standard	`-10,0`

Fabric Configuration Settings

It is important to have consistent fabric configuration settings on switches in the same fabric, since inconsistent parameters can cause fabric segmentation.

To display and check the fabric configuration settings, perform the following procedure. To troubleshoot a fabric segmentation issue, see "Restore Fabric Parameters Through ConfigUpload" on page 329.

The following parameters are included in the System Configuration Settings:

- Fabric Parameters
- Virtual Channel Settings
- Zoning Operation Parameters
- Rscn Transmission Mode

- NS Pre-zoning Mode
- Arbitrated Loop Parameters
- System Services
- Portlog Events Enable

Displaying the Fabric Configuration Settings

To display the system configuration settings:

1. Log in to the switch as admin.
2. Issue the `configshow` command. The system configuration settings appear. For example:

```
switch:admin> configshow
RSCN.end-device.TransmissionMode:0
alpaList:1
boot.device:fei
boot.file:/usr/switch/firmware
boot.gateway.ipa:192.168.147.172
boot.ipa:192.168.147.172:ffffff00
boot.mac:10:00:00:60:69:80:04:22
boot.name:ter172
boot.server.ipa:
boot.server.name:host
boot.user:user
diag.loopID:125
diag.mode.burnin:0
diag.mode.burnin.1.name:switchess.sh
diag.mode.burnin.10.name:switchess.sh
diag.mode.burnin.2.name:switchess.sh
diag.mode.burnin.3.name:switchess.sh
diag.mode.burnin.4.name:switchess.sh
diag.mode.burnin.7.name:switchess.sh
diag.mode.burnin.8.name:switchess.sh
diag.mode.burnin.9.name:switchess.sh
diag.mode.burnin.level:0
```

```
diag.mode.esd:0
diag.mode.lab:28
<output truncated>
```

Note: System configuration parameters vary depending on switch model and configuration.

Backing Up the Fabric Configuration Settings

Keep a backup file of the fabric configuration settings in the event that the configurations are lost, or unintentional changes are made.

Fabric Configurations can be saved through the Fabric OS, or through Fabric Manager. To back up or restore system configuration settings through Fabric Manager, refer to the *HP StorageWorks Fabric Manager 4.1.1 User Guide*.

To upload a backup copy of the configuration settings to a host computer:

1. Verify that the FTP service is running on the host workstation.
2. Log in to the switch as admin.
3. Issue the `configupload` command. The command becomes interactive and you are prompted for the required information. For example:

   ```
   switch:admin> configupload
   Server Name or IP Address [host]: 192.168.15.42
   User Name [user]: johndoe
   File Name [config.txt]: config-switch.txt
   Password:xxxxx
   Upload complete
   switch:admin>
   ```

Restoring the Fabric Configuration Settings

System Configurations can be restored through the Fabric OS, or through Fabric Manager. To restore system configuration settings through Fabric Manager, refer to the *HP StorageWorks Fabric Manager 4.1.1 User Guide*.

To restore the system configuration settings from a previously saved backup using Fabric OS:

1. Verify that the FTP service is running on the host workstation.

2. Log in to the switch as admin.
3. Disable the switch by issuing the `switchdisable` command.
4. Issue the `configdownload` command. The command becomes interactive and you are prompted for the required information.
5. At the `Do you want to continue [y/n]` prompt enter `y`.
6. Issue the `reboot` command to reboot the switch:

```
switch:admin> reboot
```

Swapping Port Area IDs

The port swap feature enables you two swap area IDs on two physical switch ports.

Enabling the PortSwap Feature

To enable the port swap feature:

1. Log in to the switch as admin.
2. Enable the port swap feature by issuing the command:

```
portswapenable
```

The port swap feature is enabled.

Disabling the PortSwap Feature

To disable the port swap feature:

1. Log in to the switch as admin.
2. Disable the port swap feature by issuing the command:

```
portswapdisable
```

The port swap feature is disabled.

Swapping Port Area IDs

Use this procedure to swap the port area IDs of two switch ports. To swap port area IDs, the port swap feature must be enabled, and both switch ports must be disabled. The swapped area IDs for the two ports remain persistent across reboots, power cycles, and failovers.

To swap area IDs for a pair of switch ports:

1. Log in to the switch as admin.
2. Enable the port swap feature:

   `portswapenable`
3. Disable the ports where you want to swap area IDs:

   portdisable *port1*

   portdisable *port2*
4. Swap the port area IDs:

   portswap [slot/]*port1* [slot/]*port2*

   The `slot` option is required only for switches that have slots.

   The following example shows port swapping for a SAN Switch 2/32.

   ```
   switch:admin> portswapenable
   done.
   switch:admin> portdisable 26
   switch:admin> portdisable 27
   switch:admin> portswap 26 27
   portswap done
   switch:admin>
   ```

Viewing Swapped Ports

To display swapped ports on a switch:

1. Log in to the switch as admin.
2. Verify the port area IDs have been swapped:

   `portswapshow`

   A table is displayed showing the physical port numbers and the logical area IDs for any swapped ports.

Gateway Compatibility

This section includes the following topics

- "About Gateways" on page 71
- "About ISL R_RDY Mode" on page 71

- "Enabling and Disabling ISL R_RDY Mode" on page 72

About Gateways

A gateway is a device that interconnects geographically dispersed SAN islands into a single unified fabric. A gateway provides point-to-point E_Port connectivity between two Fibre Channel switches that are separated by a protocol-independent metro or wide area network, such as IP or SONET. Except for link initialization, gateway devices are mostly transparent to switches and provide E_Port connectivity from one switch to another. When a gateway receives traffic destined for a remote device, frames may be encapsulated into the frame or packet used by the other network and then passed across the network, to be received by the switch at the remote end

About ISL R_RDY Mode

Switch ports usually initialize using Exchange Link Parameters (ELP) Mode 1; however, Gateways expect an initialization that uses ELP mode 2. Enabling ISL R_RDY mode simplifies Gateway connections by causing the port initialization to use the expected method (ELP mode 2). Therefore, the WAN gateway does not need to support a special mode for these switches.

Additional R_RDY Information

- R_RDY was first available in Fabric OS v3.1.0 and v4.1.0.
- Any number of E_Ports in a fabric can be configured for ISL R_RDY mode.
- No license is required.

Special Considerations for R_RDY Mode

- When determining switch count maximums, include the switches connected to both gateways.
- When a port is set to ISL R_RDY Mode, the port does not check FC addresses for compliance with Core PID requirements. Check Core PID settings carefully on all switches in the fabric. If Core PIDs are not consistent among the switches in the fabric, the fabric segments.
- ISL R_RDY Mode does not currently support Extended Fabrics, or the security features in Secure Fabric OS.

Enabling and Disabling ISL R_RDY Mode

Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more information about the `portcfgislmode` command.

1. (Optional) Issue the `configure` command on all switches to make sure the PID format is consistent across the entire fabric.
2. Log in as admin to the switch on which you want to configure ISL R_RDY mode.
3. Issue the `portcfgislmode [`*`slotnumber`*`/]`*`portnumber`*`, [1 | 0]` command.
   - Specify the slot number in a Core Switch 2/64 switch. The slot number must be followed by a slash (/) and the port number.
   - Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
   - Specify `1` to enable ISL R_RDY mode.
     Specify `0` to disable ISL R_RDY mode.

     This operand is required.
4. Repeat these steps for any additional ports that are to be connected to a Gateway.

Changing a Switch Name

Switches can be identified by IP address, Domain ID, WWN, or customized switch name.

To change the name of a switch:

1. Log in to the switch as admin.
2. Issue the `switchname` command:

   ```
   switchname "newname"
   ```

   where *`newname`* is the new name for the switch.

Version 4.x switch names can be 1–15 characters long, must begin with a letter, and can contain letters, numbers, or the underscore character. It is not necessary to use the quotation marks. For example:

```
switch:admin> switchname "switch62"
Committing configuration...
Done.
switch62:admin>
```

Switch Status Policies

For detailed information about setting policy parameters, refer to the *HP StorageWorks Fabric Watch 4.2.x User Guide*.

The policy parameter determines how many failed or non-operational units per contributor will trigger a status change in the switch.

Each parameter can be adjusted so that a specific threshold must be reached before that parameter changes the overall status of a switch to MARGINAL or DOWN. For example, if the FaultyPorts DOWN parameter is set to 3, the status of the switch changes if 3 ports fail. Only one policy parameter needs to pass the MARGINAL or DOWN threshold to change the overall status of the switch.

There are seven parameters that determine the status of a switch:

- Number of faulty ports
- Missing GBICs
- Power supply status
- Temperature in enclosure
- Fan speed
- Port status
- ISL status

These are discussed in the following sections.

Viewing the Policy Threshold Values

To view the switch status policy threshold values:

1. Log in to the switch as admin.
2. Issue the `switchstatuspolicyshow` command.

- For a nonmodular switch the output is similar to the following:

```
switch:admin> switchstatuspolicyshow
The current overall switch status policy parameters:
                   Down    Marginal
 ----------------------------------
      FaultyPorts  2         1
      MissingSFPs  0         0
    PowerSupplies  0         1
     Temperatures  2         1
             Fans  2         1
       PortStatus  0         0
        ISLStatus  0         0
switch:admin>
```

- For a modular switch, the output is similar to the following:

```
switch:admin> switchstatuspolicyshow
The current overall switch status policy parameters:
                   Down    Marginal
 ----------------------------------
      FaultyPorts  2         1
      MissingSFPs  0         0
    PowerSupplies  2         1
     Temperatures  2         1
             Fans  2         1
       PortStatus  0         0
        ISLStatus  0         0
               CP  0         1
              WWN  0         1
            Blade  0         1switch:admin>
```

Configuring the Policy Threshold Values

To set the switch status policy threshold values:

1. Log in to the switch as admin.

2. Issue the `switchstatuspolicyset` command. The current switch status policy parameter values are displayed.

Note: By setting the DOWN and MARGINAL value for a parameter to 0,0 that parameter is no longer used in setting the overall status for the switch.

---

3. You are prompted to enter values for each DOWN and MARGINAL threshold parameter:
   a. Enter the number of faulty ports required to change the switch status to DOWN and press **Enter**.
   b. Enter the number of faulty ports required to change the switch status to MARGINAL and press **Enter**.
   c. Enter the number of missing GBICs required to change the switch status to DOWN and press **Enter**.
   d. Enter the number of missing GBICs required to change the switch status to MARGINAL and press **Enter**.
   e. Enter the number of bad power supply warnings required to change the switch status to DOWN and press **Enter**.
   f. Enter the number of bad power supply warnings required to change the switch status to MARGINAL and press **Enter**.
   g. Enter the number of temperature warnings required to change the switch status to DOWN and press **Enter**.
   h. Enter the number of temperature warnings required to change the switch status to MARGINAL and press **Enter**.
   i. Enter the number of fan speed warnings required to change the switch status to DOWN and press **Enter**.
   j. Enter the number of fan speed warnings required to change the switch status to MARGINAL and press **Enter**.
   k. Enter the number of port down warnings required to change the switch status to DOWN and press the **Enter**.
   l. Enter the number of port down warnings required to change the switch status to MARGINAL and press **Enter**.
   m. Enter the number of ISLstatus down warnings required to change the switch status to DOWN and press **Enter**.

n. Enter the number of ISLstatus down warnings required to change the switch status to MARGINAL and press **Enter**.

For example:

```
switch:admin> switchstatuspolicyset
To change the overall switch status policy parameters
The current overall switch status policy parameters:
Down Marginal
----------------------------------
FaultyPorts 2 1
MissingSFPs 0 0
PowerSupplies 2 1
Temperatures 2 1
Fans 2 1
PortStatus 0 0
ISLStatus 0 0
Note that the value, 0, for a parameter, means that it is
NOT used in the calculation.
** In addition, if the range of settable values in the prompt is
(0..0),
** the policy parameter is NOT applicable to the switch.
** Simply hit the Return key.
The minimum number of
FaultyPorts contributing to
DOWN status: (0..32) [2] 3
FaultyPorts contributing to
MARGINAL status: (0..32) [1] 2
MissingSFPs contributing to
DOWN status: (0..32) [0]
MissingSFPs contributing to
MARGINAL status: (0..32) [0]
Bad PowerSupplies contributing to
DOWN status: (0..2) [2]
Bad PowerSupplies contributing to
```

```
MARGINAL status: (0..2) [1]
Bad Temperatures contributing to
DOWN status: (0..5) [2]
Bad Temperatures contributing to
MARGINAL status: (0..5) [1]
Bad Fans contributing to
DOWN status: (0..6) [2]
Bad Fans contributing to
MARGINAL status: (0..6) [1]
Down PortStatus contributing to
DOWN status: (0..32) [0]
Down PortStatus contributing to
MARGINAL status: (0..32) [0]
down ISLStatus contributing to
DOWN status: (0..32) [0]
down ISLStatus contributing to
MARGINAL status: (0..32) [0]
Policy parameter set has been changed
switch:admin>
```

4. Verify the threshold settings you have configured for each parameter. Issue the `switchstatuspolicyshow` command to view your current switch status policy configuration:

Tracking Switch Changes

The Track Change feature allows you to keep a record of specific changes that may not be considered switch events, but may provide useful information. The output from the track changes feature is dumped to the error log for the switch. Use the `errdump` command or `errshow` command to view the error log.

Items in the error log created from the Track changes feature are labeled `TRACK`.

Trackable changes are:

— Successful login

— Unsuccessful login

— Logout

- — Config file change from task
- — Track-changes on
- — Track-changes off

An SNMP-TRAP mode can also be enabled; refer to the `trackchangeshelp` command in the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

For troubleshooting information on the Track Changes feature, see "Inaccurate Information in the Error Log" on page 365.

Enabling the Track Changes Feature

To enable the track changes feature:

1. Log in to the switch as admin.
2. Issue the `trackchangesset 1` command to enable the track changes feature.

   A prompt is displayed, verifying that the Track Changes feature is on. For example:

   ```
   switch:admin> trackchangesset 1
   Committing configuration...done.
   switch:admin>
   ```

   The output from the track changes feature is dumped to the error log for the switch. Use the `errdump` command or `errshow` command to view the error log.

   Items in the error log created from the Track changes feature are labeled `TRACK`.

Displaying Whether the Track Changes Feature is Enabled

To display the status of the Track Changes feature:

1. Log in to the switch as admin.
2. Issue the `trackchangesshow` command.

The status of the Track Changes feature is displayed as either on or off. This also displays whether the Track Changes feature is configured to send SNMP traps. For example:

```
switch:admin> trackchangesshow
Track changes status: ON
Track changes generate SNMP-TRAP: NO
switch:admin>
```

Routing

This section discusses the following routing topics:

In-Order Delivery

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for instance, a link goes down), traffic is rerouted around the failure. When topology changes occur, some frames could be delivered out of order.

The default behavior is to automatically enable out-of-order delivery of frames during fabric topology changes. This enables fast rerouting after a fabric topology change. See "Forcing In-order Delivery of Frames" on page 80 to change the default routing settings during topology changes.

Dynamic Load Sharing

Routing is generally based on the incoming port and the destination domain. This means that all the traffic coming in from a port (either E_Port or Fx_Port) that is directed to the same remote domain is routed through the same output E_Port. To

optimize fabric routing, when there are multiple equivalent paths to a remote switch, traffic is shared among all the paths. Load sharing is recomputed when a switch is booted up or every time a change in the fabric occurs. (A change in the fabric is defined as an E_Port going up or down, or an Fx_Port going up or down.) For more information, see "Using Dynamic Load Sharing" on page 80.

Forcing In-order Delivery of Frames

To force in-order delivery of frames during fabric topology changes:

1. Log in to the switch as admin.
2. Issue the `iodset` command.

Note: Use this command with care. It can cause a delay in the establishment of a new path when a topology change occurs.

Restoring In-order Delivery of Frames

To restore the default in-order delivery setting (which allows frames to be delivered out-of-order during topology changes for faster delivery):

1. Log in to the switch as admin.
2. Issue the `iodreset` command.

Using Dynamic Load Sharing

Optimal load sharing is rarely achieved with DLS disabled. If DLS is turned on (using `dlsset`), routing changes can affect working ports. For example, if an Fx_Port goes down, another Fx_Port may be rerouted from one E_Port to a different E_Port. The switch minimizes the number of routing changes, but some are necessary to achieve optimal load sharing.

If DLS is turned off (using `dlsreset`), load sharing is performed only at boot time or when an Fx_Port comes up. To enable dynamic load sharing:

1. Log in to the switch as admin.
2. Issue the `dlsshow` command to view the current DLS setting.

   One of the following messages appears:

   - `DLS is set`

The message means that the DLS option is turned on. Load sharing is reconfigured with every change in the fabric.

- `DLS is not set`

  The message means that the DLS option is turned off. Load sharing is reconfigured only when the switch is rebooted or an Fx_Port comes up.

3. Issue the `dlsset` command to enable Dynamic Load Sharing when a fabric change occurs.
4. Issue the `dlsReset` command to disable Dynamic Load Sharing.

   Load sharing is performed only at boot time or when an Fx_Port comes up.

Viewing Routing Path Information

To view routing path information;

1. Log in as admin.
2. Issue the `topologyshow` command to display the fabric topology, as it appears to the local switch.

   The following entries appear:

   — `Local Domain` - Domain number of local switch.

   — `Domain` - Domain number of destination switch.

   — `Metric` - Cost of reaching destination domain.

   — `Name` - Name of the destination switch.

   — `Path Count` - Number of currently active paths to the destination domain.

   — `Hops` - Maximum number of hops to reach destination domain.

   — `Out Port` - The Port that the incoming frame is forwarded to, in order to reach the destination domain.

   — `In Ports` - Input ports that use the corresponding out port to reach the destination domain. This is the same information provided by `portrouteshow` and `urouteshow`.

   — `Total Bandwidth` - Maximum bandwidth of the out port.

   — `Bandwidth Demand` - Maximum bandwidth demand by the in ports.

   — `Flags` - Always `D`, indicating a dynamic path. A dynamic path is discovered automatically by the fabric shortest path first (FSPF) path selection protocol.

For example:

```
switch:admin> topologyshow
2 domains in the fabric; Local Domain ID: 1
Domain: 6
Metric: 500
Name: switch
Path Count: 4
Hops: 1
Out Port: 60
In Ports: None
Total Bandwidth: 2 Gbps
Bandwidth Demand: 0 %
Flags: D
Hops: 1
Out Port: 61
In Ports: None
Total Bandwidth: 2 Gbps
Bandwidth Demand: 0 %
Flags: D
Hops: 1
Out Port: 62
In Ports: None
Total Bandwidth: 2 Gbps
Bandwidth Demand: 0 %
Flags: D
Hops: 1
Out Port: 58
In Ports: None
Total Bandwidth: 2 Gbps
Bandwidth Demand: 0 %
Flags: D
```

3. Issue the `urouteshow [slotnumber/][portnumber] [, domainnumber]` command to display unicast routing information.

   The following entries appear:

   — `Local Domain` - Domain number of local switch.

   — `In Ports` - Port from which a frame is received.

   — `Domain` - Destination domain of incoming frame.

   — `Out Port` - Port that the incoming frame is forwarded to, in order to reach the destination domain.

   — `Metric` - Cost of reaching destination domain.

   — `Hops` - Maximum number of hops to reach destination domain.

   — `Flags` - Indicates if route is dynamic (D) or static (S). A dynamic route is discovered automatically by the FSPF path selection protocol. A static route is assigned using the command `urouteconfig`.

   — `Next (Dom, Port)` - Domain and port number of the next hop. These are the domain number and the port.

This example displays the routing information of all the active ports:

```
switch:admin> urouteshow

Local Domain ID: 3

In Port Domain Out Port Metric Hops Flags Next (Dom, Port)

---------------------------------------------------------------

0 1 11 1000 1 D 1,0

11 2 0 1500 2 D 4,0

4 0 500 1 D 4,0

16 1 27 1000 1 D 1,1

27 2 16 1500 2 D 4,16

4 0 500 1 D 4,0:
```

This example displays the routing information for port 11 on slot 1.

```
switch:admin> urouteshow 1/11
Local Domain ID: 3
In Port Domain Out Port Metric Hops Flags Next (Dom, Port)
---------------------------------------------------------------
11 2 16 1500 2 D 4,16
4 16 500 1 D 4,16
```

This example displays the routing information of port 11 to domain 4 only:

```
switch:admin> urouteshow 1/11, 4
Local Domain ID: 3
In Port Domain Out Port Metric Hops Flags Next (Dom, Port)
---------------------------------------------------------------
11 4 16 500 1 D 4,16
```

Viewing Routing Information Along a Path

To view routing information:

1. Log in as admin.
2. Issue the `pathInfo` command to display various routing-oriented information for each hop on a path.

   The following entries are displayed:

Hop	Hop number. The local switch is hop 0.
In Port	Port that the frames come in from on this path. For hop 0, the source port.
Domain ID	Domain ID of the switch.
Name	Name of the switch.
Out Port	Output port that the frames use to reach the next hop on this path. For the last hop, the destination port.
BW	Bbandwidth of the output ISL, in Gb/sec. It does not apply to the embedded port.

Cost	Cost of the ISL used by FSPF routing protocol. It applies only to an E_Port.

Paths always originate on the local switch. The path destination can be specified by domain or port. By default, the path is the path taken by traffic from the source port to destination port, but you can also specify all or portions of a path. Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for details.

Help Commands

Each Fabric OS command provides Help information that displays what the command does, explains the possible operands, displays the command level, and sometimes provides additional information.

Displaying Help Information for a Command

To display help information about a command:

1. Log in to the switch as admin.
2. Issue the `help` command using the following syntax:

   `help` *`command`*

   where *`command`* is the name of the command you would like help with.

   For example:

```
switch:admin> help configure
Administrative Commands                                    configure(1m)
NAME
     configure - change system configuration settings
SYNOPSIS
     configure
AVAILABILITY
     admin
DESCRIPTION
     This command changes some  system configuration settings,
     including:
          o Arbitrated loop settings
          o Switch fabric settings
          o System services settings
```

```
            o Virtual channel settings
<output truncated>
```

Additional Help Topics

The `help` command lists most of the help files. There are also commands that provide additional help files for specific topics. The following is not a complete list of help files:

- `diagHelp` prints diagnostic help information.
- `fwHelp` prints Fabric Watch help information.
- `licenseHelp` prints license help information.
- `perfHelp` prints Performance Monitoring help information.
- `routeHelp` prints routing help information.
- `trackChangesHelp` prints Track Changes help information.

Reading Hexadecimal Port Diagrams

Many of the commands, such as `bcastshow`, `portlogshow`, and `portlogdump`, return port diagrams in hexadecimal format.

The following example shows the `bcastshow` command and lists of `Member Ports`, `Member ISL Ports`, and `Static ISL Ports` in hexadecimal format:

```
switch:admin> bcastshow

Group   Member Ports    Member ISL Ports        Static ISL Ports

----------------------------------------------------------------
 256      0x00000000        0x00000000              0x00000000
          0x00000000        0x00000000              0x00000000
          0x00000001        0x00000000              0x00000000
0x00012083
switch:admin>
```

To read the hexadecimal port diagrams, you must convert them to binary notation. Each hexadecimal value represents four binary values. Each hexadecimal value is converted into a group of four binary bits that represent four ports, as follows (hexadecimal value = binary value):

0 = 0000

1 = 0001

2 = 0010

3 = 0011

4 = 0100

5 = 0101

6 = 0110

7 = 0111

8 = 1000

9 = 1001

A = 1010

B = 1011

C = 1100

D = 1101

E = 1110

F = 1111

After you convert the hexadecimal numbers to a binary bit map, each bit represents a port, where a value of `1` means yes and a value of `0` means no. The bit map is read from right to left; where the least significant bit represents port 0.

For example, if the member port value is displayed in hexadecimal as:

```
0x00012083
```

This corresponds to a binary bit map of the member ports as follows:

```
0000 0000 0000 0001 0010 0000 1000 0011
```

This bit map displays the member ports as ports 0, 1, 7, 13, and 16. Note that each switch has a hidden internal port (in the example above port 16) which is always a member of a broadcast group.

Standard Security in Fabric OS

3

This chapter provides information regarding security features that are standard in the Fabric OS. Refer to the *HP StorageWorks Secure Fabric OS 4.2.x User Guide* for information about licensed security features.

The following standard fabric security information is provided:

Overview

The following standard security information is specific to v4.2.x firmware.

Standard security in FOS depends on account and password management. The information in this chapter discusses security that is available without Secure Fabric OS. For information regarding Secure Fabric OS, refer to the *HP StorageWorks Secure Fabric OS 4.2.x User Guide*.

New Features

This section discusses the following topics:

Ensuring a Secure Operating System

Fabric OS v4.2.x uses Linux as the operating system in the switch. Therefore, securing the switch includes securing the underlying operating system as well.

Fabric OS uses the Berkeley `r-` commands facility to transfer data between control processors in HP StorageWorks Core Switch 2/64 and HP StorageWorks SAN Director 2/128 platforms.

The primary security concern is the use of the `.rhosts` file. All hosts listed in the.rhosts file are trusted, meaning they can log in to the switch without any authentication such as a password. The `.rhosts` file on the switch contains the IP addresses 10.0.0.5 and 10.0.0.6, which are the IP addresses of each CP in a Core Switch 2/64 and SAN Director 2/128 chassis. To prevent the use of these facilities except from the internal network, an `iptables` firewall has been implemented. This firewall isolates the external network from the internal network and does not allow execution of `r-` commands on the switch from external hosts. However, if you logged in to a switch of CP as root, you can issue `r-` commands to the other CP.

In addition, various proprietary protocols are also used over the internal CP-to-CP Ethernet. The internal Ethernet interface is considered a "trusted" interface, over which arbitrary communications may occur. To address these security concerns, the internal Ethernet interfaces were disconnected from the public Ethernet interfaces.

A packet filter is used to isolate the internal Ethernet interface. The packet filter:

- Prevents routing of packets to and from internal network
- Protects against spoofing of internal network addresses
- Blocks all incoming packets from 10.0.0.0 to 10.0.0.255
- Closes network services intended only for the internal network without changing the source code

Firewalling with `iptables`

The Linux kernel contains advanced tools for packet filtering—the process of controlling network packets as they attempt to enter, move through, and exit your system. `Iptables` are similar to `ipchains` (which were available in pre-2.4 kernels) but greatly expand on the scope and control available for filtering network packets.

For more information about configuring `iptables`, refer to the Red Hat web site:

http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/ref-guide/ch-iptables.html

About Secure Shell (SSH)

An SSH (Secure Shell) is used to support encrypted Telnet sessions to the switch (DES encryption is not supported). The default out-of-band Telnet mechanism for managing switches was deemed insecure because the passwords are sent over the wire in clear text. It is relatively easy for any network-connected system to sniff and reap these passwords for use in subsequent intrusions. In a complex enterprise network that aggregates device management into a backbone, it is difficult to prevent, or even detect, these attempts to sniff passwords. Secure Shell (SSH), is an alternative to Telnet, and uses strong encryption to prevent password sniffing and enhance the privacy of the management link.

SSH encrypts all messages, including the client sending the password at login time. This is a significant improvement over the basic `telnet` and `sectelnet`, which encrypt only the login password. The SSH package contains a daemon

(sshd) which runs on the switch, and is very similar to telnetd, except that all messages are encrypted. The SSH daemon supports a wide variety of encryption algorithms, such as Blowfish-CBC, AES, and so forth.

The daemon requires keys (public and private) for encryption. These keys are generated by a program called ssh-keygen when the openssh RPM is installed. The keys are saved to files in the /etc directory and sshd reads them on startup:

```
ssh_host_dsa_key
ssh_host_dsa_key.pub
ssh_host_rsa_key
ssh_host_rsa_key.pub
ssh, config --> configuration file sshd server
```

Supported Versions and Features:

- Officially support version 2 of the SSH protocol (ssh2). The ssh2 protocol uses DSA key for authentication. The DSA authentication key is 1024 bits.
- Run the daemon under root identity.
- Users cannot save their public keys on the switch. A password is the only method of authentication.
- The following default ciphers for session encryption are supported: AES128-CBC, 3DES-CBC, Blowfish-CBC, Cast128-CBC, and RC4.
- The following HMACs are supported: HMAC-MD5, HMAC-SHA1, HMAC-SHA1-96, HMAC-MD5-96.

Note: If you `telnet` to another machine, and then start an SSH session inside that Telnet session, the Telnet traffic is still in clear text and is not secure.

Note: The FTP protocol is not secure. When you FTP to or from the switch, the contents are in clear text. This includes the remote FTP server's login and password. This limitation affects the commands: `savecore, configupload, configdownload,` and `firmwaredownload`.

SSH Server is installed automatically with the v4.2.x firmware download and reboot of the switch. No further action is required for the SSH Server. However, the SSH Client still needs to be installed (see "Installing and Configuring a Secure Shell (SSH) Client" on page 93).

Installing and Configuring a Secure Shell (SSH) Client

The SSH Server is installed automatically with v4.2.x; use the information below to select and install the SSH Client.

Note: The SSH Client must support v2 of the SSH protocol.

There are three options for installing the SSH Client:

Note: Only F-Secure has been tested with v4.2.x.

- **F-Secure:**
  F-Secure also provides an SSH protocol that support SSH v1 and SSH v2. The documents are available for free from the http://f-secure.com web site.
- **openssh.com**:
  Openssh may also provide an appropriate SSH Client. However, any SSH client that you choose must support v2 of the SSH Protocol.
- **PuTTY**:
  PuTTY is an SSH1+SSH2 implementation; it is a free implementation of Telnet and SSH for Win32 platforms.

See "Installing and Configuring F-Secure SSH" on page 93 for installation suggestions for F-Secure.

Installing and Configuring F-Secure SSH

A 30-day free trial is available from F-Secure.com.

1. Download the SSH Client from http://www.f-secure.com/.

   You can also download free documentation.

2. Click the SSH Client icon to invoke the F-Secure Client:

   

   The F-Secure SSH Client Default Window opens (see Figure 1).

3. Click the **Quick Connect** button to open the Connect to Remote Host window.

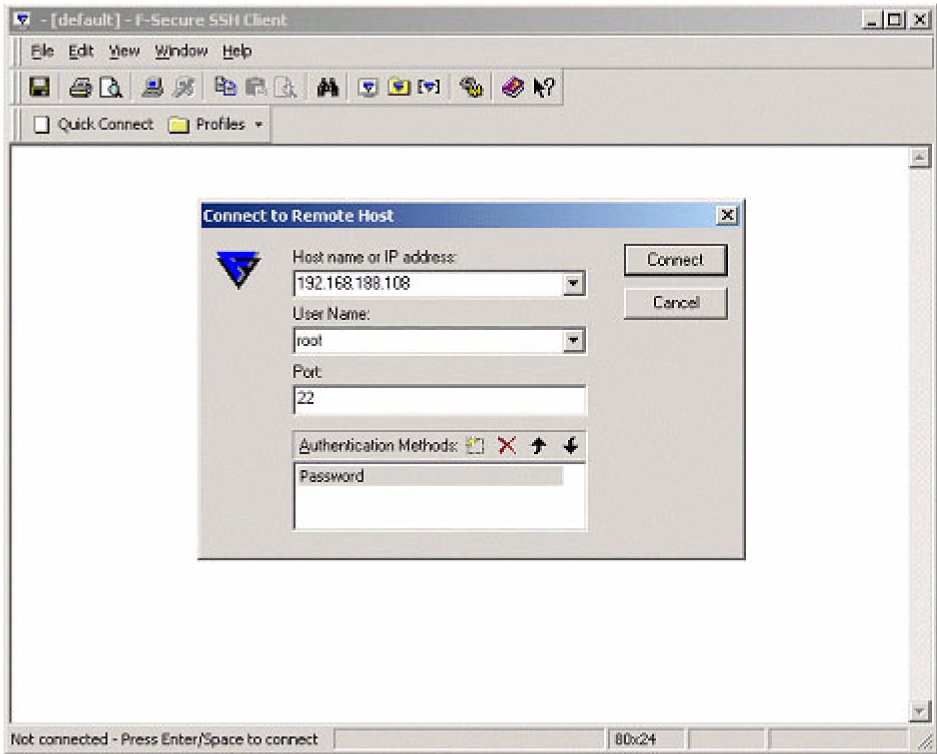

Figure 1: F-Secure SSH Connect to Remote Host Window

4. Enter the Host IP address, user name, and authentication information. Port 22 is used by SSH by default.
5. Click **Connect**. The Host Identification dialog box opens.
6. (Optional) Save the new Host Key to a local database.
7. Click **Yes** or **No**. The Password dialog box opens.
8. Enter a password. Disclaimer information displays and a session is started.

Troubleshooting the F-Secure SSH Client

If there is a malfunction or a bug in the program, a dialog box opens.

1. Select **Help** > **Troubleshooting**.
2. Select the **Copy to Clipboard** button to save any relevant information about the problem.
3. Go to http://www.f-secure.com/support.

Additional SSH Resources

Users may avail themselves of the following resources:

- *SSH, The Secure Shell: The Definitive Guide*. By Daniel J. Barrett and Richard Silverman. ISBN 0596000111.
- SSH IETF web site: http://www.ietf.org/ids.by.wg/secsh.html

Disabling the Telnet Interface

You may wish to disable Telnet to prevent a user from passing cleartext passwords over the network when logging in to the switch. The `configure [telnetd]` command is provided to let you disable the Telnet interface. The default configuration of the switch ships with Telnet enabled.

For more information on the `configure` command, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

1. Log in to the switch as admin.
2. Enter `configure [telnetd]` command and press **Enter**.

Note: This `configure` command can be run with the switch enabled.

The Telnet interface is disabled.

SNMP, HTTP, API, RSNMP, WSNMP, SES, and MS are managed through their respective policies when security is enabled. Refer to the *HP StorageWorks Secure Fabric OS 4.2.x User Guide* for information.

Listeners

Linux subsystem listeners are not needed to implement supported features, and capabilities are blocked. The listeners blocked depend on whether the switch is a Core Switch 2/64 and or a non-modular switch. Table 3 lists the blocked listeners.

Table 3: Blocked Listeners

Listener Name	Core Switch 2/64 and SAN Director 2/128	Other FOS 4.x Switches
chargen	Do not start	Do not start
echo	Do not start	Do not start
daytime	Do not start	Do not start
discard	Do not start	Do not start
ftp	Do not start	Do not start
rexec	Block with packet filter	Do not start
rsh	Block with packet filter	Do not start
rlogin	Block with packet filter	Do not start
time	Block with packet filter	Do not start
rstats	Do not start	Do not start
rusers	Do not start	Do not start

Default Fabric and Switch Accessibility

This section discusses the default fabric from the perspective of hosts, devices, switch, access, and zoning.

Hosts

- Any host can access the fabric by SNMP.
- Any host can Telnet to any switch in the fabric.
- Any host can establish an HTTP connection to any switch in the fabric.
- Any host can establish an API connection to any switch in the fabric.

Devices

- All devices can access the management server.
- Any device can connect to any FC port in the fabric.

Switch Access

- Any switch can join the fabric.
- All switches in the fabric can be accessed through the serial port.
- All switches in the fabric that have front panels (some of the HP. StorageWorks 1 GB switches) can be accessed through the front panel.

Zoning

- Node WWNs can be used for WWN-based zoning.

Passwords

This section discusses passwords in detail, covering the following topics:

- "About Passwords" on page 97
- "Comparing Password Behavior Between Firmware Versions" on page 99
- "Comparing Password Behavior Between Firmware Versions" on page 99

About Passwords

There are four accounts for each switch. For a Core Switch 2/64, this means there are four accounts for switch instance 0, and four accounts for switch instance 1. The account names are the same for both switch instances. See Table 4 and Table 5.

All account names remain the same as Fabric OS v4.0: root, factory, admin, and user.

At each account level, you can change passwords for that account and for all accounts that have lesser privileges.

Note: There is one exception to the password structure; admin level users can change the root password by entering the `passwd` root. They must also know the old root password.

Password Levels

There are four levels of account access:

- root - not recommended
- factory - not recommended
- admin- recommended for administrative operations
- user - recommended for non-administrative operations

Therefore, if you are logged in as admin, you can change the passwords for both admin and user.

Table 4: Password Accounts

Switch	Access Level	Passwords Required
One logical switch	root	one
	factory	one
	admin	one
	user	one

Because Core Switch 2/64 switches have two logical switches, and the CP blades have a set of passwords, Core Switch 2/64 switches have three sets of passwords as shown in Table 5.

Table 5: Core Switch 2/64 Switch Password Accounts

Switch	Access Level	Passwords	Password Sets
Single Core Switch 2/64			
Logical Switch 0	root	one	One set of passwords
	factory	one	
	user	one	
	admin	one	
CPs			

Table 5: Core Switch 2/64 Switch Password Accounts

Switch	Access Level	Passwords	Password Sets
Logical Switch 1	root	one	One set of passwords
	factory	one	
	user	one	
	admin	one	

Note: Record your passwords and store in a secure place, as recovering passwords may require significant effort.

Comparing Password Behavior Between Firmware Versions

The following sections provide detailed password information for v2.6/3.0, v2.6.2/3.1, v4.0 and v4.1 and later:

- "Account and Password Characteristics Matrix" on page 100
- "Password Prompting Matrix" on page 103
- "Password Recovery Options" on page 105
- "Password Migration Behavior During Firmware Upload and Download" on page 106

Password Management Information

Table 6 describes the password standards and behaviors between v2.6/3.0, v2.6.2/3.1, v4.0 and v4.1 and later.

Table 6: Account and Password Characteristics Matrix

Topic	V2.6/3.0	V2.6.2/3.1	V4.0	V4.1 and later
How many accounts are on the switch?	4	4	4, chassis based	Core Switch 2/64 - 8 for the chassis, 4 per switch: SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, SAN Director 2/128
What are the various account login names?	root, factory, admin, user	root, factory, admin, user	root, factory, admin, user	root, factory, admin, user.
Can account names be changed? (Does the `passwd` command prompt for account name changes?)	Yes, when Secure FOS is disabled; No, when Secure FOS is enabled.	Yes, when Secure FOS is disabled; No, when Secure FOS is enabled.	No	No, regardless of security mode.
What are the maximum and minimum number of characters for a password?	Minimum of 8 and maximum of 40 characters with printable ASCII.	Minimum of 8 and maximum of 40 characters with printable ASCII.	0 - 8 (Standard UNIX)	Minimum of 8 and maximum of 40 characters with printable ASCII.
Can different switch instances use a different password for the same account login level? For example, can the password for admin for switch 0 be different from the password for admin for switch 1?	N/A	N/A	No	Yes for Core Switch 2/64. N/A for all other switches.
Does the root account use restricted shell?	No	No	No	No
When logging in to a factory installed switch, do you use the default passwords?	Yes	Yes	Yes	Yes

Table 6: Account and Password Characteristics Matrix (Continued)

Topic	V2.6/3.0	V2.6.2/3.1	V4.0	V4.1 and later
Does a user need to know the old passwords when changing passwords by the `passwd` command?	Yes, the old password is required to change any password, regardless of the level at which users log in.	Yes, the old password is required to change any password, regardless of the level at which users log in.	Yes, except when "root" changes someone else's password. This is standard UNIX behavior; no additional security is enforced.	Old password is required only when changing password for the same level user password. Changing password for lower level user doesn't require old password. For example, users log in as admin; old admin password is required to change the admin password. But old user password is not required to change the user password.
Can `passwd` change higher-level passwords? For example, can admin change root password?	No. If users log in as admin, the users can change only admin and user passwords; the users cannot change factory, nor root password.	No. If users log in as admin, the users can change only admin and user passwords; the users cannot change factory, nor root password.	Yes, but asks for the old password of the higher-level account (for example, root).	Yes; if users log in as admin, they can change the root, factory, and admin passwords. However, if one logs in as user, one can change only the user password.

Table 6: Account and Password Characteristics Matrix (Continued)

Topic	V2.6/3.0	V2.6.2/3.1	V4.0	V4.1 and later
Can API change passwords?	API can change admin passwords on any switch, when security mode is disabled. It can change only the admin password on the Primary FCS switch when security mode is enabled.	API can change admin passwords on any switch, when security mode is disabled. It can change only the admin password on the Primary FCS switch when security mode is enabled.	Yes, only for admin.	Yes, only for admin.
Can Web Tools change passwords?	When security mode is disabled, users can change the admin and user passwords on all switches using Web Tools. When security mode is enabled, users can change only the admin and user passwords on the Primary FCS switch using Web Tools.	When security mode is disabled, users can change the admin and user passwords on all switches using Web Tools. When security mode is enabled, users can change only the admin and user passwords on the Primary FCS switch using Web Tools.	No	No
Can SNMP change passwords?	No	No	No	No

Password Prompting Behaviors

Table 7 describes the expected password prompting behaviors between v2.6/3.0, v2.6.2/3.1, v4.0, and v.4.1 and later.

Table 7: Password Prompting Matrix

Topic	V2.6/3.0	V2.6.2/3.1	V4.0	V4.1.0 and later
Must *all* password prompts be completed for *any* change to take effect?	Yes. If users only provide some of the passwords before exiting, no passwords are changed. Prompting continues on the next appropriate login.	Yes. If users only provide some of the passwords before exiting, no passwords are changed. Prompting continues on the next appropriate login.	No. Partial changes of all four passwords are allowed.	No. Partial changes of all four passwords are allowed.
When does the password prompt display?	When users log in as root, factory, or admin.	When users log in as root, factory, or admin.	When users log in as root, factory, or admin, the accounts with default password are prompted for change. The accounts with non-default passwords are not prompted.	When users log in as root, factory, or admin, the accounts with default password are prompted for change. The accounts with a non-default password are not prompted.
Is a user forced to answer password prompts before getting access to the firmware?	No, users can press CNTRL+C to get out of password prompting.	No, users can press CNTRL+C to get out of password prompting.	No, users can press CNTRL+C to get out of password prompting.	No, users can press CNTRL+C to get out of password prompting.
Do users need to know the old root password when answering prompting?	No	No	Yes in v4.0 *No in v4.0.2 only	No

Table 7: Password Prompting Matrix (Continued)

Topic	V2.6/3.0	V2.6.2/3.1	V4.0	V4.1.0 and later
Are new passwords forced to be set to something different than the old passwords?	Yes	Yes	Yes	Yes
Is password prompting disabled when security mode is enabled?	Yes	Yes	Yes	Yes
Is the `passwd` command disabled until the user has answered password prompting?	True	True	False	True
Does password prompting reappear when passwords are changed back to default using the `passwd` command?	No	No	Yes	No
Does password prompting reappear when passwords are changed back to default using the `passwdDefault` command?	Yes	Yes	Yes	Yes.

Password Recovery Options

Table 8 describes the options available when one or more types of passwords are lost.

Table 8: Password Recovery Options

Topic	V2.6/3.0	V2.6.2/3.1	V4.0	V4.1.0 and later
If all the passwords are forgotten, what is the password recovery mechanism? Are these procedures non-disruptive?	The user has to get special password recovery firmware based on the WWN of the switch from Tech Support, and then download the special firmware; this resets all passwords to default.The procedures are disruptive.	The user has to get a special password recovery firmware based on the WWN of the switch from Tech Support, and then download the special firmware; this resets all passwords to default.The procedures are disruptive.	Contact Technical Support. A non-disruptive procedure is available.	Contact Technical Support. A non-disruptive procedure is available.
If a user has only the root password, what is the password recovery mechanism?	Option 1: Use `passwd` command to set other passwords. Option 2: Use `passwdDefault` command to set all passwords to default.	Option 1: Use `passwd` command to set other passwords. Option 2: Use `passwdDefault` command to set all passwords to default.	Root can change any password by using the `passwd` command.	Use `passwd` command to set other passwords.
How to recover boot PROM password?	N/A	N/A	N/A	Contact Technical Support. See "About Boot PROM Passwords" on page 109 to set the boot PROM and recovery passwords.
How does the user recover a user, admin, or factory password?	See "Recovering a User, Admin, or Factory Password" on page 115.	See "Recovering a User, Admin, or Factory Password" on page 115.	See "Recovering a User, Admin, or Factory Password" on page 115.	See "Recovering a User, Admin, or Factory Password" on page 115.

Password Migration During Firmware Upgrade and Downgrade

Table 9 describes the expected outcome of password settings when upgrading or downgrading firmware for v2.6 and v3.0, v2.6.2 and v3.1, v4.0 and v.41.

Table 9: Password Migration Behavior During Firmware Upload and Download

Topic	V2.6/3.0	V2.6.2/3.1	V4.0x	V4.1.0 or later
When upgrading to a newer firmware release for the first time, which passwords are used?	For first time firmware upgrades from v2.4.x to v2.6.0x, the v2.4.x passwords are preserved.	For first time firmware upgrades from v3.0.x to v3.1.2, the v3.0.x passwords are preserved.	N/A	For first time firmware upgrades from v4.0.x to v4.2.x, the v4.0.x passwords are preserved.
Which passwords are preserved during subsequent firmware upgrades?	For second firmware upgrades (and each subsequent upgrade) from v2.4.x to v2.6.0x, the passwords that were last used in v2.6.0x are effective.	For second firmware upgrades (and each subsequent upgrade) from v3.0.x to v3.1, the passwords that were last used in v3.1 are effective.	N/A	For second firmware upgrades (and each subsequent upgrade) from v4.0.x to v4.2.x, the passwords that were last used in v4.0.x are effective.
Is downgrading to an older firmware version (which does not support Secure Fabric OS) allowed when security mode is enabled?	Yes. FirmwareDownload does not prevent such downgrades.	Yes	N/A	Yes
Which passwords are used if downgrading to an older firmware for the first time?	When downgrading firmware from v2.6.0x to v2.4.x for the first time, the default passwords are used.	When downgrading firmware from v3.1.2 to v3.0.x for the first time, the default passwords are used.	N/A	If the switch had v4.2.x factory installed, a firmware downgrade from v4.2.x to v4.0.x uses the default passwords.

Table 9: Password Migration Behavior During Firmware Upload and Download (Continued)

Topic	V2.6/3.0	V2.6.2/3.1	V4.0x	V4.1.0 or later
When downgrading to an older firmware at subsequent times, which passwords are used?	Firmware downgrades from v2.6 to v2.4 use the previous v2.4 passwords (the passwords used before the firmware had been upgraded to v2.6).	Firmware downgrades from v3.1 to v3.0 use the previous v3.0 passwords (the passwords used before the firmware had been upgraded to v3.1).	Firmware downgrades within 4.x use the old 4.0 passwords.	Firmware downgrades from v4.2.x to v4.0.x use the previous v4.0.x passwords (the passwords used before the firmware had been upgraded to v4.2.x).
When downgrading and then upgrading, what passwords are used?	When upgrading firmware for a second time, the old v2.6 or v3.1 passwords are used (the passwords used before the firmware had been downgraded).	When upgrading firmware for a second time, the old v2.6 or v3.1 passwords are used (the passwords used before the firmware had been downgraded).	When upgrading firmware for a second time, the old passwords are used (the passwords used before the firmware had been downgraded).	When upgrading firmware for a second time, the old passwords are used (the passwords used before the firmware had been downgraded). For 4.0.x to 4.2.x, use the 4.0.x passwords

Modifying a Password

There are four levels of account access. See "About Passwords" on page 97. To bypass the password prompt without completing the prompts, press **CTRL+C**.

1. Create a CLI connection to the switch.
2. Log in using the account for which you want to change the password.

   At each account level, you can change passwords for that account and all accounts that have lesser privileges. See "About Passwords" on page 97.
3. Issue the `passwd` command and enter the requested information at the prompts.

   You must enter the current password for the first account. Passwords do not have to contain uppercase, lowercase, or non-alphanumeric characters.

Note: If you are using Secure Fabric OS, new passwords are saved and distributed to all the switches in the fabric.

To change a password:

```
cp0 login: admin
Password:
sec51_switch0:admin> passwd
Changing password for admin
Enter old password:
Enter new password:
Re-type new password:
Changing password for user
Enter new password:
Re-type new password:
```

4. Repeat for all switches in the fabric.

Note: You cannot change account login names in Standard or Secure Mode.

Setting Recovery Passwords

This section discusses the following:

- "About Boot PROM Passwords" on page 109
- "Setting Both the Boot PROM and the Recovery Passwords (SAN Switch 2/32)" on page 109
- "Setting Both the Boot PROM and Recovery Passwords (Core Switch 2/64 and SAN Director 2/128)" on page 110
- "Setting the Boot PROM Password Only (SAN Switch 2/32)" on page 111
- "Setting the Boot PROM Password Only (Core Switch 2/64 and SAN Director 2/128)" on page 113
- "About Forgotten Passwords" on page 114
- "Recovering a User, Admin, or Factory Password" on page 115

- "Recovering a Forgotten Root or Boot PROM Password" on page 115

About Boot PROM Passwords

Fabric OS v4.2.x provides the option of setting the Boot PROM and Recovery passwords. This option does not apply to Fabric OS v3.1.2 or v2.6.2.

The Boot PROM and Recovery passwords provide an additional layer of security beyond the root password.

- Setting a Boot PROM password protects the boot prompt from unauthorized use.
- Setting a Recovery password turns on the password recovery option, which requires a user to contact Technical Support before recovering a root or boot PROM password.

Note: HP strongly recommends setting both the Boot PROM and Recovery passwords on all switches running Fabric OS v4.2.x. Not setting either of these passwords can compromise fabric security.

Setting Both the Boot PROM and the Recovery Passwords (SAN Switch 2/32)

Note: Setting the Boot PROM and Recovery passwords requires accessing the boot prompt, which stops traffic flow through the switch until the switch is rebooted.

---

1. Connect to the serial port interface as described in step 1 of "Setting the Boot PROM Password Only (SAN Switch 2/32)" on page 111.
2. Reboot the switch.
3. Press **ESC** within four seconds after the message `Press escape within 4 seconds` displays.

   The following options are available:

   — Start system.

   — Recovery password.

   — Enter command shell.

4. Enter 2 at the prompt to set the Recovery password. The following message displays: `Recovery password is NOT set. Please set it now.`
5. Enter the Recovery password. The Recovery password must be between 8 and 40 alphanumeric characters. HP recommends a random password that is 15 characters or longer for higher security. The firmware prompts for this password only once. It is not necessary to remember the Recovery password.

   The prompt for the Boot PROM password displays `New password:`.
6. Enter the Boot PROM password, then reenter when prompted. Record this password for future use. The new passwords are automatically saved (the `saveenv` command is not required).
7. Reboot the switch. Traffic flow resumes when the switch finishes rebooting.

Setting Both the Boot PROM and Recovery Passwords (Core Switch 2/64 and SAN Director 2/128)

The Boot PROM and Recovery passwords must be set for each CP card on a Core Switch 2/64.

1. Connect to the serial port interface on the standby CP card, as described in step 1 of "Setting the Boot PROM Password Only (Core Switch 2/64 and SAN Director 2/128)" on page 113.
2. Log in to the active CP card by serial or Telnet and issue the `hadisable` command to prevent failover during the remaining steps.
3. Reboot the standby CP card by pressing the yellow ejector buttons at top and bottom of the CP card, then pressing both ejector handles back towards the switch to lock the card back into the slot.
4. Press **ESC** within four seconds after the message `Press escape within 4 seconds` displays.

   The following options are available:

   — Start system.

   — Recovery password.

   — Enter command shell.
5. Enter 2 at the prompt to set the Recovery password. The following message displays: `Recovery password is NOT set. Please set it now.`

6. Enter the Recovery password. The Recovery password must be between 8 and 40 alphanumeric characters. HP recommends a random password that is 15 characters or longer for higher security. The firmware prompts for this password only once. It is not necessary to record the Recovery password.

   The `New password` prompt displays.
7. Enter the Boot PROM password, then reenter when prompted. Record this password for future use. The new passwords are automatically saved (the `saveenv` command is not required).
8. Fail over the active CP card by issuing the `hafailover` command. Traffic flow through the active CP card resumes when the failover is complete.
9. Connect the serial cable to the serial port on the new standby CP card (previous active CP card).
10. Repeat step 2 through step 7 for the new standby CP card (each CP card has a separate Boot PROM password).
11. Log in to the active CP card by serial or Telnet and issue the `haenable` command to restore high availability.

Setting the Boot PROM Password Only (SAN Switch 2/32)

The option of setting the Boot PROM password is available only on a SAN Switch 2/32 and Core Switch 2/64, but is not recommended. See "Setting Both the Boot PROM and the Recovery Passwords (SAN Switch 2/32)" on page 109.

Note: Setting the Boot PROM password requires accessing the boot prompt, which stops traffic flow through the switch until the switch is rebooted.

---

1. Create a serial connection to the switch, as shown below. If Secure Mode is enabled, connect to the Primary FCS switch. If the switch does not have a serial port, contact Technical Support.
   a. Connect the serial cable to the serial port on the switch and to an RS-232 serial port on the workstation.

      If the serial port on the workstation is RJ-45 instead of RS-232, remove the adapter on the end of the serial cable and insert the exposed RJ-45 connector into the RJ-45 serial port on the workstation.
   b. Disable any serial communication programs running on the workstation.

c. Open a terminal emulator application (such as HyperTerminal on a PC, or TERM or Kermit in a UNIX environment), and configure the application as follows:

— In a Windows 95, 98, 2000, or Windows NT environment:

ParameterValue

Bits per second: 9600

Databits: 8

Parity: None

Stop bits: 1

Flow control: None

— In a UNIX environment, enter the following string at the prompt:

```
tip /dev/ttyb -9600
```

2. Reboot the switch by issuing the `reboot` command.
3. Press **ESC** within four seconds after the message `Press escape within 4 seconds` displays.

   The following options are available:

   — Start system.

   — Recovery password.

   — Enter command shell.
4. Enter `3` at the prompt to enter the command shell.
5. Issue the `passwd` command at the prompt.

Note: This command is specific to the Boot PROM password when entered from the boot interface.

6. Enter the Boot PROM password at the prompt, then reenter when prompted. The password must be eight alphanumeric characters (any additional characters are not recorded).
7. Record this password for future use.
8. Issue the `saveenv` command to save the new password.

9. Reboot the switch by issuing the `reset` command.
   Traffic flow resumes when the switch finishes rebooting.

Setting the Boot PROM Password Only (Core Switch 2/64 and SAN Director 2/128)

The option of setting the Boot PROM password is available only on a SAN Switch 2/32, Core Switch 2/64 and SAN Director 2/128, but is not recommended. See "Setting Both the Boot PROM and Recovery Passwords (Core Switch 2/64 and SAN Director 2/128)" on page 110.

On the Core Switch 2/64, the suggested procedure is to set the password on the standby CP, then fail over; then set the password on the previously Active (now Standby) CP to minimize disruption to fabric.

The Boot PROM and Recovery passwords must be set for each CP card on a Core Switch 2/64 switch.

Note: Setting the Boot PROM password requires accessing the boot prompt, which stops traffic flow through the switch until the switch is rebooted.

---

1. For the SAN Director 2/128, determine the active CP card by opening a Telnet session to either CP card, logging in as admin, and issuing the `hashow` command.
2. Log in to the active CP card by serial or Telnet and issue the `hadisable` command to prevent failover during the remaining steps.
3. Create a serial connection to the standby CP card as described in "Setting the Boot PROM Password Only (SAN Switch 2/32)" on page 111.
4. Reboot the standby CP card by pressing the yellow ejector buttons at top and bottom of the CP card, then pressing both ejector handles back towards the switch to lock the card back into the slot. This causes the card to reset.
5. Press **ESC** within four seconds after the message `Press escape within 4 seconds` displays.

   The following options are available:

   — Start system.

   — Recovery password.

   — Enter command shell.
6. Enter `3` at the prompt to enter the command shell.

7. Issue the `passwd` command at the prompt.

Note: This command is specific to the Boot PROM password when entered from the boot interface.

---

8. Enter the Boot PROM password at the prompt, then reenter when prompted. The password must be eight alphanumeric characters (any additional characters are not recorded).
9. Record this password for future use.
10. Issue the `saveenv` command to save the new password.
11. Reboot the standby CP card by issuing the `reset` command.
12. Fail over the active CP card by opening a Telnet session to the active CP card, logging in as admin, and issuing the `hafailover` command.
    Traffic resumes flowing through the newly active CP card after it has completed rebooting.
13. Connect the serial cable to the serial port on the new standby CP card (previous active CP card).
14. Repeat step 3 through step 11 for the new standby CP card (each CP card has a separate Boot PROM password).
15. Log in to the active CP card by serial or Telnet and issue the `haenable` command to restore high availability.

About Forgotten Passwords

Passwords can be recovered as follows:

- If the user, admin, or factory passwords are lost, but the root password is known, follow the steps described in "Recovering a User, Admin, or Factory Password" on page 115.
- If the root or boot PROM password is lost, contact Technical Support.

Recovering a User, Admin, or Factory Password

The user, admin, and factory passwords can be recovered if the root password is known. The following procedure applies to all switch types and Fabric OS versions.

1. Open a CLI connection (serial or Telnet) to the switch. If the Secure Mode of the Secure Fabric OS feature is enabled, connect to the Primary FCS switch.
2. Log in as root.
3. Enter the command corresponding to the type of password lost:
   - passwd user
   - passwd admin
   - passwd factory
4. Enter the requested information at the prompts.

Recovering a Forgotten Root or Boot PROM Password

To recover a lost Boot PROM password, contact Technical Support.

Frequently Asked Questions About Changing Passwords

Q: How many characters can a password have?

A: Passwords can have a minimum of 8 and a maximum of 40 characters. The password must contain two of the following classes: upper and lower case letters, numerals, and non-alphanumeric characters.

Q: Do new passwords have to be set to something different than the old password or the default password?

A: Yes

Q: Does the user have to know the old password when changing passwords using the `passwd` command?

A: The user is prompted to use the old password when the account is being changed or has the same or higher privilege than the login account. For example, if the login account is admin, the old admin password is required to change the admin password. But the old user password is not required for the admin account to change the user account password except when it is initially changed.

Q: Can the `passwd` command change higher-level passwords? For example, can admin level change root level passwords?

A: Yes. If end-users log in as admin, the end-user can change root, factory, and admin passwords. However, if you log in as user you can change only the user password. To change a higher level account, you must provide the higher level account's old password.

Q: Can Web Tools change passwords?

A: No

Q: Can SNMP change passwords?

A: No

Q: When is the user prompted to change the password?

A: When you first log in as root, factory, or admin, you are prompted to change the password, if the password is still default. Accounts with non-default passwords are prompted.

Q: Do users need to know the old root password when answering prompting?

A: No

Q: Is password prompting disabled when security mode is enabled?

A: Yes

4 Downloading Firmware

This chapter provides information on upgrading firmware on the Fabric OS v4.x switches. It also provides basic information on upgrading firmware using Web Tools and Fabric Manager.

This chapter discusses the following major topics:

About Firmware Upgrades

This section discusses the firmware upgrade process.

Understanding the Dual-CP Firmware Upgrade Process

Fabric OS v4.1.0 and later offer a non-disruptive firmware download process for the HP StorageWorks SAN Switch 2/32 and the HP StorageWorks Core Switch 2/64.

The following process describes the default behavior of the `firmwaredownload` command on a Core Switch 2/64 dual CP when no options are used. See "Upgrading Firmware on the SAN Switch 2/32" on page 120 or "Upgrading Firmware on the Core Switch 2/64" on page 125 for instructions.

Note: Step 1 is executed on the active CP by the operator. Steps 2 thorough 6 are performed automatically for the operator.

---

1. The `firmwaredownload` command is executed.
2. Firmware download is done on the standby CP first.
3. The Standby CP forces a failover.
4. Firmware download is completed on the "new" standby CP.
5. The "new" standby is rebooted.
6. The `firmwareCommit` command is executed on both CPs. The `firmwaredownloadstatus` command shows the firmware process. The entire firmware activation process may take 20 to 25 minutes.

   If there is a problem, wait for the timeout. By design, partitions are made equal in the event of a firmware download failure.
7. If an error is encountered during the `firmwaredownload` (such as an unexpected power outage), the command ensures that both partitions of a CP contain the same version of firmware. However, partitions in a different CP may contain different versions of firmware. In that event, rerun the firmware download command.

Non-Disruptive Firmware Activation

Fabric OS v4.1.0 and later provide the ability to activate firmware non-disruptively.

The Core Switch 2/64 Platform provides non-disruptive behavior as long as both CP blades are installed and are fully synchronized. Issue the `haShow` command to confirm synchronization.

Core Switch 2/64 With Only 1 CP

The Core Switch 2/64 needs to reboot itself to activate firmware. The process is disruptive. It is identical to the version 4.0.2 single CP firmware activation.

SAN Switch 2/32

During a firmware upgrade, the firmware fails over to itself. However, the process takes longer because a reboot of the operating system is required.

Firmware Compatibility

Table 10 provides information about upgrading from one specific firmware version to another on the Core Switch 2/64.

Table 10: Firmware Compatibility for the Core Switch 2/64

Current Firmware (From)	Desired Firmware (To)	Where to Execute	OK to Use Web Tools?	Command
v4.0.2d	v4.2.x	On Active CP (manages both CPs)	Yes	`firmwaredownload`

Table 11 provides information about upgrading from one specific firmware version to another on the SAN Switch 2/32.

Table 11: Firmware Compatibility for the SAN Switch 2/32

Current Firmware (From)	Desired Firmware (To)	Where to Execute	OK to Use Web Tools?	Command
v4.0.2d	v4.2.x	SAN Switch 2/32	Yes	`firmwaredownload`

Performing Firmware Upgrades

This section provides the following firmware upgrade instructions:

- "Upgrading Firmware on the SAN Switch 2/32" on page 120
- "Upgrading Firmware on the SAN Switch 2/32 After v4.1.0" on page 124
- "Upgrading Firmware on the Core Switch 2/64" on page 125

Upgrading Firmware on the SAN Switch 2/32

The SAN Switch 2/32 maintains a primary and secondary partition for firmware. The `firmwaredownload` command downloads only to the secondary partition. The `firmwaredownload` command also has an auto-commit option (which is the default) that automatically commits the firmware to both partitions during the download process. If you override the auto-commit option (on the command line), you must execute this command on the SAN Switch 2/32 manually (not recommended for normal operation). After a reboot, the partitions are swapped.

Use the following procedure to download and commit a new firmware version to both partitions of flash memory.

To upgrade or restore the switch firmware:

1. Consider the current firmware version of the switch.
   - If the switch is already running firmware v4.1.0 or later, specific fabric configuration factors should be considered for neighboring switches. See "Upgrading Firmware on the SAN Switch 2/32 After v4.1.0" on page 124.
   - If the switch is running firmware that is earlier than v4.1.0, go to step 2.
2. Verify that the FTP service is running on the host workstation (or on a Windows machine).
3. Log in to the switch as the admin user.
4. Enter the following command (double quotes are optional in v4.x firmware):

   ```
   firmwaredownload "hostIPaddr", "user", "path_filename",
   "password"
   ```

   - *hostIPaddr* is the IP address of the host computer.
   - *user* is the user ID used to log in to this computer.
   - *path_filename* is the path location and filename of the new firmware file.

- *password* is the password for the user ID specified. (Note: the password can be NULL)

5. Enter Y for yes to continue with the reboot, when prompted. Or issue the firmwaredownload command to be prompted for parameters.

   During a Non-Disruptive FirmwareDownload and Activation on the SAN Switch 2/32, the SAN Switch 2/32 uses a Proxy Application Standby Service in place of a Standby CP to facilitate the FirmwareDownload process. This service sends HA State in sync or HA State out of Sync messages as a result.

Example Displays a “prompted” firmware download.

```
switch:admin> firmwaredownload
Server Name or IP Address: 192.168.166.30
User Name: johndoe
File Name: /fw/4.2.x/release.plist
Password: xxxxxx
Full Install (Otherwise upgrade only) [Y]:
Do Auto-Commit after Reboot [Y]:
Reboot system after download [N]:
You can run firmwareDownloadStatus to get the status
of this command.

This command will cause the switch to reset and will
require that existing telnet, secure telnet or SSH
sessions be restarted.

Do you want to continue [Y]: y
Firmwaredownload has started.
dir ##################################################
terminfo ##################################################
<output truncated>
glibc ##################################################
sin ##################################################
Write kernel image into flash.

All packages have been downloaded successfully.
Firmwaredownload has completed successfully.
HA Rebooting ...
FVT226_19:admin> Loopback backup before go standby
 0x220 (fabos):  Switch: 0, Info FSSME-HA_IN_SYNC, 4, HA State is in sync!
 0x220 (fabos):  Switch: 0, Info FSSME-HA_OUTOF_SYNC, 4, HA State out of sync!

sysctrld: all services Standby
System Restart After HA reboot
sysctrld: all services Standby
loopback replay before go active
0x220 (fabos):  Switch: 0, Info FSSME-HA_IN_SYNC, 4, HA State is in sync!
0x220 (fabos):  Switch: 0, Info FSSME-HA_OUTOF_SYNC, 4, HA State out of sync!

Firmwarecommit has started.
Doing firmwarecommit now.
Please wait ...

Replicating kernel image.
................
Firmwarecommit has completed successfully.
file verification SUCCEEDED
Firmwaredownload command has completed successfully.
```

6. (Optional) Open another Telnet session and enter the `firmwaredownloadstatus` command to monitor the firmwaredownload status.

   The switch reboots and starts the `firmwarecommit` command after the firmware is downloaded.

Example

```
switch:admin> firmwaredownloadstatus
[0]: Tue Jan 28 10:32:34 2003
cp0: Firmwaredownload has started.

[1]: Tue Jan 28 10:36:07 2003
cp0: Firmwaredownload has completed successfully.

[2]: Tue Jan 28 10:57:09 2003
cp0: Firmwarecommit has started.

[3]: Tue Jan 28 10:36:07 2003
cp0: Firmwarecommit has completed successfully.

[4]: Tue Jan 28 11:03:28 2003
cp0: Firmwaredownload command has completed successfully.

switch:admin>
```

7. Issue the `firmwareshow` command after the switch reboots and the `firmwarecommit` finishes.

   The firmware level is displayed for both partitions.

Example

```
switch:admin> firmwareshow
Local CP (Slot 5, CP0): Active
        Primary partition: v4.2.x
        Secondary Partition: v4.2.x
Remote CP is Non-redundant.
switch:admin>
```

Note: Subsequent upgrades to the v4.1.0 or later firmware require the following fabric configuration: all adjacent switches must be running firmware v2.6.1, v3.1, or v4.1.0 or later (as appropriate to the hardware type). See "Upgrading Firmware on the SAN Switch 2/32 After v4.1.0" on page 124.

Upgrading Firmware on the SAN Switch 2/32 After v4.1.0

After the SAN Switch 2/32 has been upgraded to firmware v4.1.0 for the first time, subsequent firmware downloads (to v4.1.0 or later) require a specific fabric configuration of neighboring switches.

Fabric Configuration of Switches Directly Connected to the SAN Switch 2/32

Before upgrading a SAN Switch 2/32 switch that is *already* running v4.1.0 or later, all directly-connected switches must be running one of the following firmware versions (as appropriate to the hardware type):

- 2.6.1 or later
- 3.1.0 or later
- 4.1.0 or later

Due to the hot code activation feature of the SAN Switch 2/32 beginning with Fabric OS v4.1.0 (and later), switches that are directly connected to the SAN Switch 2/32 during any subsequent firmware download must be running the firmware listed above. If adjacent switches are running older firmware, the adjacent switches run the risk of timing-out during subsequent firmware upgrades of the SAN Switch 2/32.

Example Scenario

1. Current setup:

   A SAN Switch 2/32 has been upgraded, and has been running v4.1.0 or later.

   Three switches are directly connected to this SAN Switch 2/32:

   — One switch is running 2.6.0.

   — One switch is running v3.0.2.

   — One switch is running v4.1.0.

2. Planned Change:

A user plans to upgrade the SAN Switch 2/32 to a firmware version of v4.1.0 or later

or

A user plans to redownload the v4.1.0 firmware to the SAN Switch 2/32.

3. Recommended Action:

   Before the SAN Switch 2/32 is upgraded to v4.1.0 or later (see step 2):

   — The v2.6.0 firmware should be upgraded to 2.6.1 (or later).

   — The v3.0.2 firmware should be upgraded to v3.1.0 (or later).

   — The v4.1.0 firmware can be run as-is with the SAN Switch 2/32 during the subsequent download.

Upgrading Firmware on the Core Switch 2/64

Note: The procedure below applies only to upgrading firmware from versions v4.0.0d or later.

The following firmware upgrade process is specific to the Core Switch 2/64.

The Core Switch 2/64 has four IP addresses: one for each switch (switch 0 and switch 1) and one for each of the two CPs (CP0 in slot 5 and CP1 in slot 6).

When upgrading the firmware in the Core Switch 2/64, the `firmwaredownload` command automatically loads new firmware in to both the Active CP and Standby CP; this is the default behavior in v4.1.0 and later, and no special actions are required.

To upgrade the firmware on a Core Switch 2/64:

1. Verify that the FTP service is running on the host workstation (or on a Windows machine).
2. Telnet to the Core Switch 2/64 as the admin user.
3. Telnet to either logical switch 0 or 1:

   `Telnet` *`ip address`*

4. Issue the `haShow` command to determine which CP is the Active, and which is the Standby.

Also, confirm that the two CPs are in sync. CPs must be in sync to provide the non-disruptive download.

Example:

```
switch:admin> hashow
Local CP (Slot 6, CP1): Active
Remote CP (Slot 5, CP0): Standby
HA Enabled, Heartbeat up, HA State is in Sync
```

This message varies, depending on the operating system you are currently running. In this example the Active CP is CP1, and the Standby CP is CP0.

5. Issue the `ipaddrshow` command to determine the IP address of the Active CP.

Example

```
switch:admin> ipaddrshow
       Switch number [0 for switch0, 1 for switch1, 2 for CP0, 3 for CP1, 4 for all
IP
       addresses in system]: 3
       CP1
       Ethernet IP Address: 192.168.186.196
       Ethernet Subnetmask: 255.255.255.0
       HostName : cp1
       Gateway Address: 192.168.186.1
       switch:admin>
```

6. Log in to the Active CP as the admin user.
7. Issue the following (double quotes are optional in 4.x firmware):

   `firmwaredownload “hostIPaddr”, “user”, "path_filename”, “password”`

   - `hostIPaddr` is the IP address of the host computer.
   - `user` is the user ID used to log in to this computer.
   - `path_filename` is the path location and filename of the new firmware file.
   - `password` is the password for the user ID specified. (Note: the password can be NULL)

   or

   Issue the `firmwaredownload` command to be prompted for parameters.

8. Enter `Y` for yes to continue with the reboot, when prompted.

   The firmware is downloaded onto both CPs, one at a time. During the process, the active CP is rebooted and existing services may be disrupted momentarily.

Example **Displays a prompted `firmwaredownload`**

```
switch:admin> firmwaredownload
This command will upgrade both CPs in the switch. If you
what to upgrade a single CP only, please use -s option.

You can run firmwareDownloadStatus from a telnet session
to get the status of this command.

This command will cause the active CP to reset. This will
cause disruption to devices attached to both switch 0 and
switch 1 momentarily and will require that existing telnet
sessions be restarted.

Do you want to continue [Y]: y
Server Name or IP Address: 192.168.174.91
User Name: johndoe
File Name: /fw/v4.2.x/release.plist
Password:*****
FirmwareDownload has started on Active CP. It may take up to 10 minutes.

Please use firmwareShow to see the firmware status.
```

9. Issue the `firmwaredownloadstatus` command in a new session to monitor the firmwaredownload status.

   After the firmware is downloaded, a firmware commit is started on both CPs and both partitions.

Example

```
switch:admin> firmwaredownloadstatus
[0]: Tue Mar 11 15:18:56 2003
cp0: Firmwaredownload has started on Standby CP. It may take up to 10 minutes.

[1]: Tue Mar 11 15:24:17 2003
cp0: Firmwaredownload has completed successfully on Standby CP.

[2]: Tue Mar 11 15:24:19 2003
cp0: Standby CP reboots.

[3]: Tue Mar 11 15:27:06 2003
cp0: Standby CP booted up.

[4]: Tue Mar 11 15:29:01 2003
cp1: Active CP forced failover succeeded. Now this CP becomes Active.

[5]: Tue Mar 11 15:29:05 2003
cp1: Firmwaredownload has started on Standby CP. It may take up to 10 minutes.

[6]: Tue Mar 11 15:34:16 2003
cp1: Firmwaredownload has completed successfully on Standby CP.

[7]: Tue Mar 11 15:34:19 2003
cp1: Standby CP reboots.

[8]: Tue Mar 11 15:36:59 2003
cp1: Standby CP booted up with new firmware.

[9]: Tue Mar 11 15:37:04 2003
cp1: Firmwarecommit has started on both Active and Standby CPs.

[10]: Tue Mar 11 15:42:48 2003
cp1: Firmwarecommit has completed successfully on Active CP.

[11]: Tue Mar 11 15:42:49 2003
cp1: Firmwaredownload command has completed successfully.
```

10. Issue the `firmwareshow` command to display the new firmware versions.

Example

```
switch:admin> firmwareshow
Local CP (Slot 5, CP0): Active
           Primary partition: v4.2.x
           Secondary Partition: v4.2.x
Remote CP (Slot 6, CP1): Standby
           Primary partition: v4.2.x
           Secondary Partition: v4.2.x

switch:admin>
```

Customizing the Firmware Download Process

Read "Firmware Download Requirements and Limitations" on page 140 before performing your firmware download.

The `firmwaredownload` command can be executed with options on the command line using the following format:

`firmwaredownload` -[*option*(s)]

Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more information.

Single CP Option

Use the `-s` option to enable Single CP Mode. In the Core Switch 2/64 and the SAN Switch 2/32, single CP mode lets you upgrade a single CP and select Full-install, Auto-reboot, and Auto-commit.

Note: When upgrading firmware v4.0.0c or less to v4.1.0 or later, contact your service provider.

Auto-Reboot Option

After downloading firmware, the system must be rebooted. If this option is not specified, you must issue the `reboot` command manually to activate the downloaded image. If Auto-reboot Mode is enabled, the switch reboots automatically after the `firmwaredownload` command has been run.

Use the *-b* option to enable Auto-reboot Mode.

Auto-Commit Option

By default, after running `firmwaredownload` and after `reboot`, the switch performs a `firmwarecommit` command automatically. When Auto-commit Mode is disabled, you must issue the `firmwarecommit` command manually to replicate the downloaded image from the primary partition to the secondary partition of a CP.

Use the *-n* option to chose to commit the firmware manually.

Upgrading Firmware on a Single CP (on a Core Switch 2/64)

Note: Though it is possible to download firmware to one CP at a time, is not recommended. HP recommends that both CPs be upgraded at the same time so they are consistent. You should use the following procedure only if instructed to do so by your service provider.

The following procedure enables Single Mode on a Core Switch 2/64. Single Mode lets you:

- Upgrade to a single CP on a Core Switch 2/64.
- Select a Full-install, Auto-reboot, and Auto-commit (only the `-s` option is required on the command line).

To enable Single Mode on a Core Switch 2/64:

1. Telnet in to the Core Switch 2/64 as admin.

Note: In this example, the Active CP is CP1, and the Standby CP is CP0.

---

2. Issue the `hashow` command to determine which CP is the Active and which is the Standby.

Example

```
switch:admin> hashow
Local CP (Slot 5, CP0): Active
Remote CP (Slot 6, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State in sync
```

This message varies, depending on the version of firmware that is currently installed.

3. Telnet to the Standby CP.

Example

```
Telnet 192.168.174.91
```

4. Issue the `firmwaredownload -s` command to upgrade a new version of the firmware to the Standby CP.

   The `-s` option lets you upgrade to a single CP on a Core Switch 2/64,and select a Full-install, Auto-reboot, and Auto-commit. Place a space between the command and the option.

Example

```
switch: admin> firmwaredownload -s
Server Name or IP Address: 192.158.174.91
User Name:Admin
File Name:/fw/v4.2.x/release.plist
Password:*****
```

5. Enter the user name and the Host IP (FTP server).
6. Answer the prompts as they appear. The following are the recommended responses:
   - Answer `Y` (yes) to Full Install. Answering `no` to this prompt can cause problems with the CP.
   - Answer `Y` (yes) to Auto Commit if you want the firmware to be committed automatically after download. If you answer `no`, you must manually enter the `firmwarecommit` command.
   - Answer `Y` (yes) to reboot the system after download if you want to enable Auto-reboot.

Example

```
Full Install (Otherwise upgrade only) [Y]: Y
Do Auto Commit after reboot [Y]: Y
Reboot system after download [N]: Y
```

The standby CP reboots. If the Auto-reboot option was not selected at the prompt, you must manually reboot.

7. Wait for the firmware download to complete. Issue the `firmwareDownloadStatus` command in a new session to check the status.
8. Issue the `hafailover` command to invoke a failover of the standby CP.
9. Wait for the two CPs to come back into sync (issue the `hashow` command to verify).
10. Repeat the firmware download procedure on the new standby CP when the process is completed on the first CP.

Upgrading the Firmware Advanced Using Web Tools

To upgrade the firmware using Advanced Web Tools, perform the following steps:

1. Launch Advanced Web Tools.
2. Access the Switch Admin window (see Figure 2).
3. Enter the admin user name and password.
4. Click the **Upload/Download** tab.
5. Click the **Firmware Download** radio button.
6. Select the FTP transfer protocol from the drop-down menu. FTP is the only supported transfer protocol in Fabric OS v4.1.0 or later.
7. Enter the user name, password, and host IP information.
8. Enter the fully qualified path to the firmware file.
9. Click **Apply**.

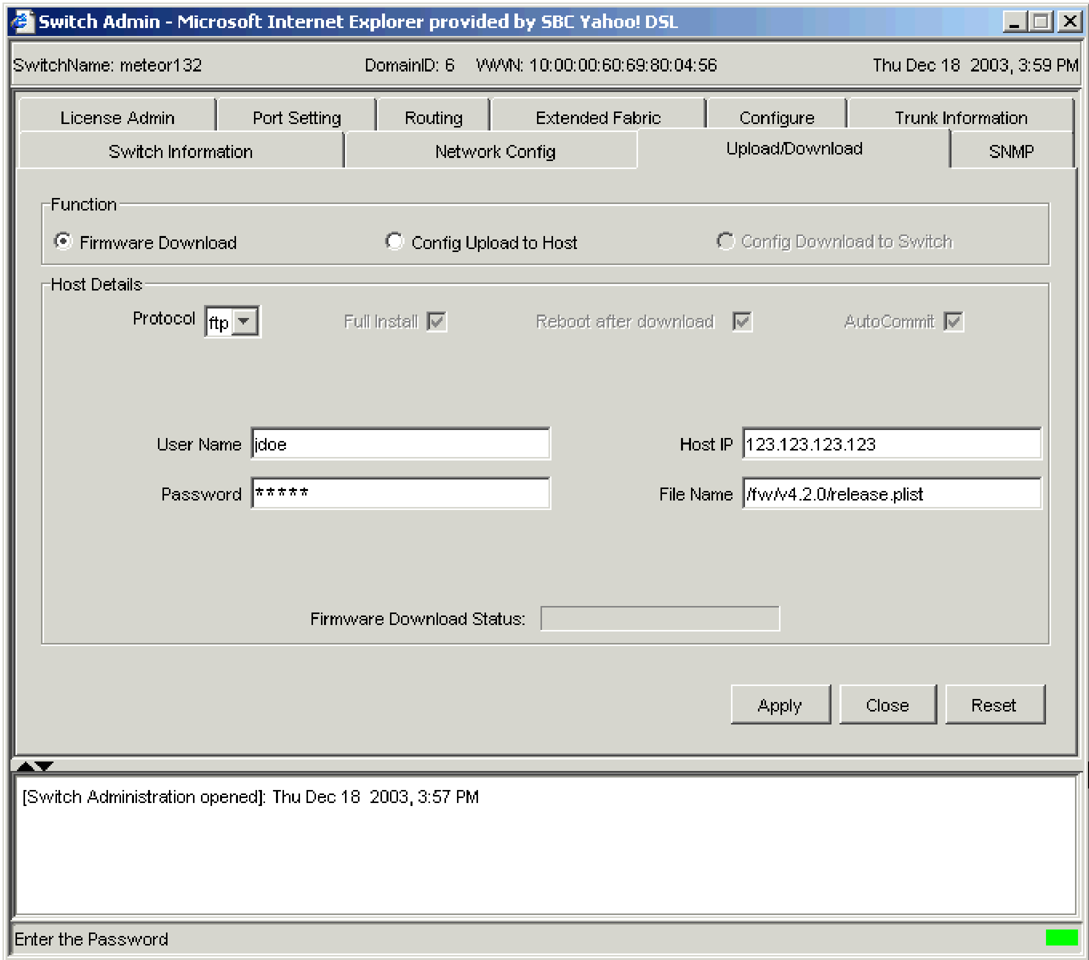

Figure 2: Web Tools Switch Admin Window

Upgrading Firmware to Multiple Switches

Simultaneously Upgrading Firmware to multiple switches requires using Fabric Manager, which is an optionally licensed software.

Before you upgrade firmware to multiple switches, verify that setup meets the following requirements:

- You have the Fabric Manager software.
- All switches that you choose to upgrade can run the firmware that you plan to download.
- All switches that you choose to simultaneously reboot reside on the same fabric.

To use Fabric Manager to concurrently download firmware to multiple switches and (optionally) reboot the switches simultaneously, follow these steps:

1. Launch the Fabric Manager software.
2. Log-on to the switches that you want to upgrade.

   For more information, refer to the *HP StorageWorks Fabric Manager 4.1.1 User Guide*.
3. From the **Tools** menu, select **Firmware download to switches** The Firmware download to switches window opens. This window is displayed in Figure 3.

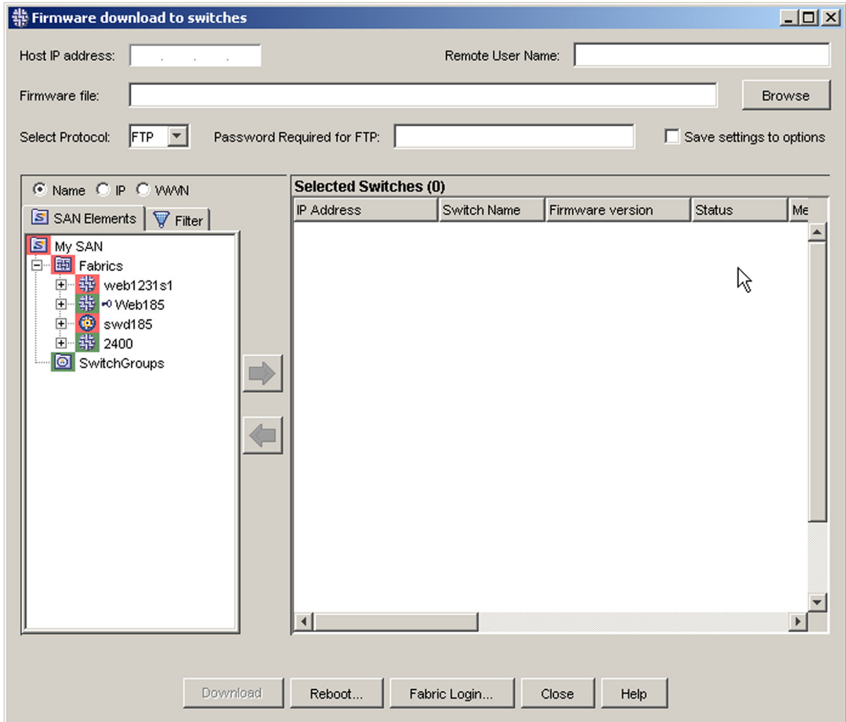

Figure 3: Firmware download to switches window

4. In the **Host IP address** field, enter the IP address of the FTP server with the firmware file.

Note: The IP address appears automatically if you have already configured file transfer options.

For more information, refer to the *HP StorageWorks Fabric Manager 4.1.1 User Guide*. If you have not configured file transfer options, check the **Save settings to options** checkbox to save your FTP settings as your file transfer options.

Note: You must click **Download** to commit the file transfer options. If for any other reason you close this window, the file transfer options do not apply.

5. In the **Remote User Name** field, enter your user ID for the FTP server.
6. In the **Firmware file** field, enter the path and name of the firmware file (in UNIX format), or click **Browse** to navigate to the file.
7. From the **Select Protocol** pulldown menu, select **FTP**.
8. In the **Password Required for FTP** field, enter your password.
9. From the **SAN Elements** tab, select the switches that you want to upgrade and move them to the Selected Switches window. You can:
   - Navigate to a switch, click the switch, then click the right-pointing arrow.
   - Click and drag a switch from the **SAN Elements** tab to the Selected Switches window.
   - Press and hold **CTRL**, click multiple switches, and click the right-pointing arrow.
   - Press and hold **CTRL**, click multiple switches, and click and drag the switches from the **SAN Elements** tab to the Selected Switches window.
   - Click and drag a fabric to the Selected Switches window to move or add all of the switches in that fabric to the Selected Switches window.

Note: You can perform a multiple switch firmware download to a maximum of five switches running versions of Fabric Manager earlier than 4.1.0

If you want to download firmware to a dual switch chassis, you can download firmware only to one logical switch at a time. Furthermore, you can download firmware only to one logical switch in a dual-switch chassis. If you add both of the logical switches in a chassis to the Selected Switches window, you receive an error prompt when you click **download**.

10. Click **Download**.
11. When the download completes, click **Reboot** to open the Sequenced Reboot window.

Note: If the switch loses network connectivity during the firmware download from Fabric Manager, the download times out after 25 minutes for switches running firmware v2.x/3.x, and after 80 minutes for switches running firmware v4.x. No error message is returned when the firmware download process gets interrupted.

Troubleshooting Firmware Download on a Core Switch 2/64

A firmware download can fail for many reasons, such as a failed network connection, a failed FTP server, or an incorrect path to the firmware file. The following are three failure scenarios:

Scenario 1
In most cases the firmware is not affected. Make corrections as necessary (check the Ethernet cables, check the file paths, and so on), and try the download again.

Scenario 2
In some cases, the firmware download process may have begun, but the firmware automatically restores itself in the event of a failure. Try the download again.

Scenario 3
In certain situations (such as a a Network connection failure or a power outage), the firmware download failure may occur at a time that leaves the Core Switch 2/64 with a different version of firmware on each CP.

Whatever the suspected cause of a firmwaredownload failure, HP recommends that you check to make sure that both CPs have the same version of firmware (use the `firmwareshow` command). If the two CPs have different firmware, use the following procedure to correct the problem.

Troubleshooting an Incomplete Firmwaredownload

1. Issue the `firmwareshow` command.

Example

```
switch: admin> firmwareshow
Local CP (Slot 5, CP0): Active
           Primary partition: v4.0.2d
           Secondary Partition: v4.0.2d
Remote CP (Slot 6, CP1): Standby
           Primary partition: v4.2.x
           Secondary Partition: v4.2.x

switch: admin>
```

   In the example above, the Active CP has the old version of firmware; the Standby CP has the new version.

2. Decide which firmware version you want to be applied to both CPs. In other words, decide whether you want to continue with the upgrade, or downgrade back to the old firmware.

   For this scenario, assume you are continuing with the upgrade to the newer firmware.

3. Telnet into the CP that contains the firmware you do *not* want.

   For this example you would Telnet into CP0, which contains the *old* firmware.

4. Issue the `firmwaredownload -s` command to download firmware to the single CP.

Example

```
switch: admin> firmwaredownload -s
Server Name or IP Address: 192.158.174.91
User Name:Admin
File Name:/fw/v4.2.x/release.plist
Password:*****
```

5. Enter the user name and the Host IP (FTP server).

6. Answer the prompts as they appear. The following are the recommended responses:
   - Answer `Y` (yes) to Full Install. Always answer `Y` to this prompt, unless specifically requested by Technical Support.
   - Answer `Y` (yes) to Auto Commit if you want the firmware to be committed automatically after download. If you answer `No`, you must manually enter the `firmwarecommit` command.
   - Answer `Y` (yes) to reboot the system after download if you want to enable Auto-reboot.

Example

```
Full Install (Otherwise upgrade only) [Y]: Y
Do Auto Commit after reboot [Y]: Y
Reboot system after download [N]: Y
```

   The standby CP reboots. If the Auto-reboot option was not selected at the prompt, you must manually reboot.

7. Wait for the firmware download to complete and then issue the `firmwareDownloadStatus` command in a new session to check the status.

Example

```
FirmwareDownload has started on Active CP. It may take up to 10 minutes.

Please use firmwareShow to see the firmware status.
switch:admin> firmwareshow
Local CP (Slot 6, CP1): Active
        Primary partition:      v4.2.x
        Secondary Partition:    v4.2.x
Remote CP (Slot 5, CP0): Standby

        Primary partition:      v4.2.x
        Secondary Partition:    v4.2.x
switch:admin>
```

8. Issue the `hafailover` command to invoke a failover of the standby CP.
9. Wait for the two CPs to come back into sync (use the `hashow` command to verify).

Firmware Download Requirements and Limitations

This section contains important information to be considered before performing your firmware download.

SAN Switch 2/32

After the SAN Switch 2/32 has been upgraded to v4.1.0 or later, all neighboring switches should be upgraded to v2.6.1, v3.1.0, or v4.1.0 *before an additional download is performed* on the SAN Switch 2/32. See "Upgrading Firmware on the SAN Switch 2/32 After v4.1.0" on page 124.

During a non-disruptive firmware download and activation of the SAN Switch 2/32, the SAN Switch 2/32 uses a Proxy Application Standby Service in place of a Standby CP to facilitate the firmware download process. As a result, this service sends `HA State in sync` or `HA State out of Sync` messages. The HA messages are normal output, and indicate that the firmware download is proceeding as expected.

Core Switch 2/64

When you are upgrading from firmware versions 4.0.0c or earlier, contact your service provider.

If the firmware download is disrupted, it is possible for the partitions in the two CPs to have different versions. When disrupted, `firmwaredownload` ensures that both partitions on the same CP have the same version, but it cannot ensure that all four partitions across both CPs have the same version.

If a firmware download is disrupted before it is complete (for example, by doing a failover in the middle of firmware download), issue the `firmwareshow` command to determine what firmware is on each CP. If the CPs have different versions, run the firmware download procedure again.

Do not perform a firmware download while the switch is running `POST`. If a firmware download is attempted on Core Switch 2/64 while `POST` is running, it may fail because the CPs cannot synchronize.

Frequently Asked Questions About Passwords, Upgrades, and Downgrades

Q: When the user upgrades to a newer firmware release for the first time, which passwords are used?

A: When you upgrade from v4.0.x to v4.1.0 or later for the first time, the v4.0.x passwords are preserved.

Q: When the user upgrades to a newer firmware release at subsequent times, which passwords are used?

A: When you upgrade from v4.0.x to v4.1.0 or later for a second time and after, the passwords that were used the last time in v4.1.0 are effective.

Q: When the user downgrades to an older firmware release for the first time, which passwords are used?

A: When you downgrade from v4.1.0 or later to v4.0.x, the default passwords are used, if v4.1 is already installed.

Q: When the user downgrades to an older firmware at subsequent times, which passwords are used?

A: When you downgrade from v4.1.0 or later to v4.0.x, the previous passwords from v4.0.x before the firmware upgrade to v4.1.0 are used.

Q: Is the user forced to answer password prompts before gaining access to the firmware?

A: No. You can bypass the password prompting by using **CTRL-C** or by pressing **Enter** after each prompt.

Working with the Core Switch 2/64 and SAN Director 2/128

5

This chapter provides information on working with the HP StorageWorks Core Switch 2/64 and HP StorageWorks SAN Director 2/128. For detailed information about the Core Switch 2/64, refer to the *HP StorageWorks Core Switch 2/64 Installation Guide*. For detailed information about the SAN Director 2/12,8 refer to the *HP StorageWorks SAN Switch 2/8V and 2/16V Installation Guide.*

Ports on the Core Switch 2/64 and SAN Director 2/128

In previous versions of the Fabric OS (v2.x and v3.x), the primary method for identifying a port within the fabric was the domain-port combination.

The following example shows the `zoneadd` command, where a port is identified using the domain and port number.

Example

```
switch:admin> zoneadd 1, 30
```

The former method of specifying a particular port cannot be used in the Core Switch 2/64 and SAN Director 2/128 because of the addition of slots and the variable number of ports within a given domain.

It was replaced in Fabric OS v4.x by two methods to specify a particular port:

- The slot/port method
- The port area number method. The port area method is used only when implementing zoning commands.

About the Slot/Port Method

A new method of specifying ports is required in the Core Switch 2/64 and SAN Director 2/128. To select a specific port you must identify both the slot number and port number you are working with.

When specifying a particular slot and port for a command, the slot number operand must be followed by the slash (/), and then a value for the port number. The following example shows how to enable port 4 on a switch blade in slot 2.

Example

```
switch:admin> portenable 2/4
```

Note: No spaces are allowed between the slot number, the slash (/), and the port number.

The Core Switch 2/64 and SAN Director 2/128 each has 10 slots:

- Slot numbers 5 and 6 are control processor cards
- Slots 1 through 4 and 7 through 10 are port cards.

- On each switch card, there are 16 ports, counted from the bottom 0 to 15. A port must be represented by both slot number (1 through 10) and port number (0 through 15).

The Core Switch 2/64 is divided into two logical switches, where slots 1 through 4 are logical switch 0, and slots 7 through 10 are logical switch 1. Typically you must be logged in to the logical switch that represents the slot where you want to execute a command. This is not true for the SAN Director 2/128, which is a single switch.

About the Port Area Number Method

Some commands, such as the Zoning commands, require you to specify ports using the Area Number method. In Fabric OS v4.*x*, each port on a particular domain is given a unique Area ID. How the port number is related to the Area ID depends upon the PID format used in the fabric.

When Core PID mode is in effect, the Area ID for port 0 is 0, for port 1 is 1, and so forth. When Enhanced Edge PID mode is in effect, the Area ID is the port number plus 16 for ports 0 through 115. For port numbers higher than 115, the Area ID wraps around, with port 116 having an Area ID of 0.

The Core Switch 2/64 chassis contains two logical switches. When using Core PID mode, the Area IDs for both logical 64-port switches range from 0 to 63. This means that both logical switch 0 and logical switch 1 have a port that is referenced with Area ID 0. Using the Enhanced Edge PID format, each logical switch has the Area IDs ranging from 16 to 79.

An Area ID for each port is unique inside each logical switch (that is, each assigned domain ID). These are two of the three parts of a 24-bit Fibre Channel Address ID: 8-bit Domain ID, 8-bit Area ID, and 8-bit Port ID.

Issue the `switchshow` command to display all ports on the current (logical) switch and their corresponding Area IDs.

Determining the Area Number (ID) of a Port

To determine the Area ID of a particular port:

1. Log in to the switch as admin.
2. Issue the `switchshow` command. This command displays all ports on the current (logical) switch and their corresponding Area IDs.

Example

```
switch:admin> switchshow
switchName:     switch
switchType:     10.1
switchState:    Online
switchRole:     Subordinate
switchDomain:   97
switchId:       fffc61
switchWwn:      10:00:00:60:69:80:04:5a
switchBeacon:   OFF
blade1 Beacon:  OFF
blade3 Beacon:  OFF

Area Slot Port Gbic Speed State
=====================================
  0    1    0   id    N2   No_Light
  1    1    1   id    N2   No_Light
  2    1    2   --    N2   No_Module
  3    1    3   id    N2   Online    E-Port  10:00:00:60:69:80:04:5b "ulys62" (T
runk master)
  4    1    4   id    N2   No_Light
  5    1    5   id    N2   Online    E-Port  10:00:00:60:69:00:54:e9 "san78" (up
stream)(Trunk master)
  6    1    6   id    N2   No_Light
  7    1    7   id    N2   No_Light
  8    1    8   --    N2   No_Module
  9    1    9   id    N2   No_Light
 10    1   10   id    N2   Online    E-Port  10:00:00:60:69:90:02:5e "sqad120" (
Trunk master)
 11    1   11   --    N2   No_Module
 12    1   12   id    N2   No_Light
 13    1   13   --    N2   No_Module
 14    1   14   id    N1   Online    F-Port  21:00:00:e0:8b:03:70:b1
 15    1   15   id    N2   Online    E-Port  10:00:00:60:69:90:02:5e "sqad120" (
Trunk master)
 32    3    0   id    N2   No_Light
 33    3    1   --    N2   No_Module
 34    3    2   id    N2   Online    Loopback->Slot  3 Port  2
 35    3    3   id    N2   No_Light
 36    3    4   id    N2   No_Light
 37    3    5   id    N2   Online    E-Port  10:00:00:60:69:00:54:ea "san79" (Tr
unk master)
 38    3    6   id    N2   No_Light
 39    3    7   id    N2   No_Light
 40    3    8   id    N2   Online    E-Port  (Trunk port, master is Slot  3 Port
   9)
 41    3    9   id    N2   Online    E-Port  10:00:00:60:69:80:04:5b "ulys62" (T
runk master)
 42    3   10   id    N2   Online    E-Port  (Trunk port, master is Slot  3 Port
   9)
 43    3   11   id    N2   Online    E-Port  (Trunk port, master is Slot  3 Port
   9)
 44    3   12   id    N2   No_Light
 45    3   13   id    N2   No_Light
 46    3   14   id    N2   No_Light
 47    3   15   id    N2   No_Light
switch:admin>
```

Basic Blade Management

For the purposes of this section, Basic Blade Management refers to:

- "Disabling a Blade" on page 147
- "Enabling a Blade" on page 147
- "Powering On a Blade" on page 148
- "Powering Off a Blade" on page 148

Disabling a Blade

One reason to disable a blade is to perform diagnostics. When diagnostics are executed manually (from the Fabric OS command line), many commands require the blade to be in an offline state. This ensures that the diagnostic does not interfere with or disturb normal fabric traffic. If the blade is not in an offline state (bladedisable), the `diagnostic` command does not run, and may display an error message.

To disable a blade:

1. Log in to the switch as admin.
2. Issue the `slotoff` command:

   `slotoff` *`slotnumber`*

   where *`slotnumber`* is the slot number of the blade you want to disable.

Example

```
switch:admin> slotoff 3

Slot 3 is being disabled
switch:admin>
```

Enabling a Blade

To enable a blade:

1. Log in to the switch as admin.
2. Issue the `sloton` command:

   `sloton` *`slotnumber`*

   where *`slotnumber`* is the slot number of the blade you want to enable.

Example

```
switch:admin> sloton 3

Slot 3 is being enabled
switch:admin>
```

Powering On a Blade

To provide power to a blade:

1. Log in to the switch as admin.
2. Issue the `slotpoweron` command:

   `slotpoweron` *`slotnumber`*

   where *`slotnumber`* is the slot number of the blade you want to power on.

Example

```
switch:admin> slotpoweron 3

Powering on slot 3
switch:admin>
```

Powering Off a Blade

To power off a blade:

1. Log in to the switch as admin.
2. Issue the `slotoff` command.

Note: The blade must be disabled so that processing stops. See "Disabling a Blade" on page 147.

---

3. Issue the `slotpoweroff` command:

   `slotpoweroff` *`slotnumber`*

   where *`slotnumber`* is the slot number of the blade you want to power off.

Example

```
switch:admin> slotpoweroff 3

Slot 3 is being powered off
switch:admin>
```

Chassis Information

For a Core Switch 2/64, the chassis-wide commands display or control both logical switches.

Displaying the Status of All Slots in the Chassis

To display the status of slots in the chassis:

1. Log in to the switch as admin.
2. Issue the `slotshow` command. This command displays the current status of each slot in the system.

   The format of the display includes a header and four fields for each slot. The fields and their possible values are:

Slot	Displays the physical slot number.
Blade Type	Displays the blade type: • SW BLADE The blade is a Switch. • CP BLADE The blade is a Control Processor. • UNKNOWN Blade not present or its type is not recognized.
ID	Displays the hardware ID of the blade type.

Status	Displays the status of the blade:

- VACANT
  The slot is empty.
- INSERTED, NOT POWERED ON
  The blade is present in the slot but is turned off.
- DIAG RUNNING POST1
  The blade is present, powered on, and running the post initialization power on self tests.
- DIAG RUNNING POST2
  The blade is present, powered on, and running the post initialization power on self tests.
- ENABLED
  The blade is on and enabled.
- DISABLED
  The blade is powered on but disabled.
- FAULTY
  The blade is faulty because an error was detected.
- UNKNOWN
  The blade is inserted but it's state cannot be determined.

Note: SAN Director 2/128 CP blades have two sections that can fail independently. A blade can still be the active blade and the switch can continue to function if one section fails. So a blade can be both active and showing a status of FAULTY.

Example

```
switch:admin> slotshow

Slot   Blade Type   ID    Status
---------------------------------
  1      SW BLADE    2      ENABLED
  2      UNKNOWN            VACANT
  3      SW BLADE    2      ENABLED
  4      UNKNOWN            VACANT
  5      CP BLADE    1      ENABLED
  6      CP BLADE    1      ENABLED
  7      UNKNOWN            VACANT
  8      SW BLADE    2      ENABLED
  9      SW BLADE    2      ENABLED
 10      SW BLADE    2      ENABLED

switch:admin>
```

Displaying Information on Switch FRUs

For complete information about switch FRUs, refer to the *HP StorageWorks Core Switch 2/64 Installation Guide* or the *HP StorageWorks SAN Director 2/128 Installation Guide*.

To view switch FRU information for a switch:

1. Log in to the switch as admin.
2. Issue the `chassisshow` command. This command displays the field replaceable unit (FRU) header content for each object in the chassis. This command returns information for each FRU, including:
   - Object ID and object number. Valid values include the following: CHASSIS, FAN, POWER SUPPLY, SW BLADE (switch), CP BLADE (control processor), WWN, or UNKNOWN. The object number refers to the slot number for blades, and unit number for everything else.
   - FRU header version number
   - Object's power consumption, positive for power supplies, negative for consumers
   - Part number (up to 14 characters)
   - Serial number (up to 12 characters)
   - Date the FRU was manufactured

- Date the FRU header was last updated.
- Cumulative time, in days, that the FRU has been powered on
- Current time, in days, since the FRU was last powered on
- Externally supplied ID (up to 10 characters)
- Externally supplied part number (up to 20 characters)
- Externally supplied serial number (up to 20 characters)
- Externally supplied revision number (up to 4 characters)

Example: See below.

```
switch:admin> chassisshow
SW BLADE  Slot: 1
Header Version:         2
Power Consume Factor:   -180
HP Part Num:       65-0000555-04
HP Serial Num:     FQ000000000
Manufacture:            Day:  5  Month:  9  Year: 2001
Update:                 Day: 18  Month:  9  Year: 2002
Time Alive:             228 days
Time Awake:             0 days
SW BLADE  Slot: 3
Header Version:         2
Power Consume Factor:   -180
HP Part Num:       65-0000555-04
HP Serial Num:     FQ000000000
Manufacture:            Day: 10  Month:  9  Year: 2001
Update:                 Day: 18  Month:  9  Year: 2002
Time Alive:             218 days
Time Awake:             0 days
CP BLADE  Slot: 5
Header Version:         2
Power Consume Factor:   -40
HP Part Num:       65-0000555-04
HP Serial Num:     FQ000000000
Manufacture:            Day:  3  Month:  5  Year: 2002
Update:                 Day: 18  Month:  9  Year: 2002
Time Alive:             51 days
Time Awake:             0 days
CP BLADE  Slot: 6
Header Version:         2
Power Consume Factor:   -40
HP Part Num:       65-0000555-04
HP Serial Num:     FQ000000000
Manufacture:            Day: 26  Month:  1  Year: 2002
Update:                 Day: 18  Month:  9  Year: 2002
Time Alive:             131 days
Time Awake:             0 days
SW BLADE  Slot: 8
Header Version:         2
Power Consume Factor:   -180
HP Part Num:       65-0000555-04
HP Serial Num:     FQ000000000
Manufacture:            Day: 22  Month:  9  Year: 2001
Update:                 Day: 18  Month:  9  Year: 2002
Time Alive:             217 days
Time Awake:             0 days

<output truncated>
```

Setting the Blade Beacon Mode

When beaconing mode is enabled, the port LEDs flash amber in a running pattern from port 0 through port 15 and back again. The pattern continues until the user turns it off. This can be used to signal the user regarding a particular blade.

To set the blade beacon mode on:

1. Log in to the switch as admin.
2. Issue the `bladebeacon` command:

   `bladebeacon` *`slotnumber`*`,` *`mode`*

   where *`slotnumber`* is the blade where you want to enable beacon mode; *mode* 1 turns beaconing mode on; *mode* 0 turns beaconing mode off.

Example

```
switch:admin> bladebeacon 3, 1
switch:admin>
```

Distributed Fabrics Procedures

6

This chapter provides information on procedures for the Remote Switch and the Extended Fabric features, using Fabric OS commands. These features require a license key to activate.

This chapter has the following information:

License Activation

Use the `licenseshow` command to verify that the Remote Switch and the Extended Fabric license keys are installed to your switch. See "Managing Licensed Features" on page 39 for more information on activating a feature using license keys.

Configuring a Remote Switch Fabric

HP Remote Switch can be used for any gateway device, including Fibre Channel over ATM, Fibre Channel over IP, Fibre Channel over SONET, and Fibre Channel over DWDM. Most of these gateway devices include a large number of buffers to cover data transfer over a WAN. The HP StorageWorks switches on each side of the gateway must have identical configurations. Only active SFPs should be used when using HP Remote Switch.

Remote Switch is automatically activated when you enable the licence key. The only required action is to connect the fabrics through the gateway device, and make sure that the `configure` command parameters are compatible with the gateway device.

You may be required to reconfigure the following parameters, depending on the gateway requirements:

- R_A_TOV: Specify a Resource Allocation Timeout Value compatible with your gateway device.
- E_D_TOV: Specify an Error Detect Timeout Value compatible with your gateway device
- Data field size: Specify the maximum Fibre Channel data field reported by the fabric. Verify the maximum data field size the network-bridge can handle. Some bridges may not be able to handle a maximum data field size of 2112.
- BB credit: Specify the number of Buffer-to-Buffer credits for Nx_port devices.
- Suppress Class F Traffic: Use this parameter to disable class F traffic. Some network-bridge devices may not have a provision for handling class F frames. In this case, transmission of class F frames must be suppressed throughout the entire Remote Switch fabric.

Modifying Configuration Parameters

To set the access and reconfigure these parameters:

1. Log in to the switch as admin.
2. Issue the `switchdisable` command to disable the switch.
3. Issue the `configure` command.
4. Enter `yes` at the `Fabric Parameters` prompt.
5. Press **Enter** to scroll through the Fabric Parameters without changing their values, until you reach the parameter you want to modify.
6. Specify a new parameter value that is compatible with your gateway device.
7. Press **Enter** to scroll through the remainder of the configuration parameters. Make sure that the configuration changes are committed to the switch.
8. Repeat for all switches in the fabrics to be connected through a gateway device. These parameters must be identical on each switch in the fabric, and between fabrics connected through the gateway device.

Example:

The following example shows how to modify the Data Field Size and Suppress Class F Traffic parameter settings on a switch.

```
switch:admin> switchdisable
switch:admin> configure

Configure...

Fabric parameters (yes, y, no, n): [no] yes

    Domain: (1..239) [3]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    Data field size: (256..2112) [2112] 1000
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0] 1
    VC Encoded Address Mode: (0..1) [0]
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]
    BB credit: (1..16) [16]

  Virtual Channel parameters (yes, y, no, n): [no]
  Zoning Operation parameters (yes, y, no, n): [no]
  RSCN Transmission Mode (yes, y, no, n): [no]
  NS Operation Parameters (yes, y, no, n): [no]
  Arbitrated Loop parameters (yes, y, no, n): [no]
  System services (yes, y, no, n): [no]
  Portlog events enable (yes, y, no, n): [no]
Committing configuration...done.
switch:admin>
```

Configuring an Extended Fabric ISL Link

Issue the `portcfglongdistance` command to configure extended fabric ISL links (see "Configuring a Long Distance Connection" on page 159 next, for details), but first note the following:

- Do not configure an extended fabric ISL link with v2.x switches in any fabric with 3.x or 4.x switches; however, v2.x switches can be in a fabric with extended fabric ISL links configured between any combination of 3.x and 4.x switches.
- Do not set the long distance fabric `fabric.ops.mode.longDistance` parameter in fabrics where extended fabrics ports are configured only on v3.x or v4.x switches.
- The long distance ISL ports must have the same configuration, or the fabric will segment.

Configuring a Long Distance Connection

Note: ISL Trunking is not supported on a long distance ISL

This procedure is used to configure the ports in a long distance ISL connection. Both ports must be configured to the same distance level. Only active SFPs should be used when using HP Extended Fabric.

To configure the distance level for an Extended Fabric ISL port:

1. Log in to the switch as admin.
2. Issue the following command:

```
portcfglongdistance [slot/]port
[distance_level][vc_translation_link_init]
```

where:

slot	Specifies the slot number in an HP StorageWorks Core Switch 2/64. This option is not applicable to any other switch type. The slot number must be followed by a slash (/) and the port number.
port	Specifies the port number where you want to initiate the long distance ISL connection.
distance_level	Indicates the long distance mode to be set on the port.

vc_translation_link_init
Enables the long-distance link initialization sequence.By default this option is set to 0 (disabled).

The next example shows a configuration for the LD distance level.

Example:

```
switch:admin> portcfglongdistance 1/1 LD 1
switch:admin>
```

Select from the following port levels:

Normal E_port	This is the standard default value of all ports on the switch. Normal E_port – supports up to 10 km at 1 G and up to 5 km at 2 G. This operation is sometimes referred to as *L0* in documents. L0 and normal E_ports are the same.
Fx	F_port or FL_port.
Level E (LE)	An Extended Fabric license is not required. Supports up to 10 km at both 1 G and 2 G. This mode was created to support 2 G up to 10 km and uses EF principles. This mode does not support trunking with other ports.
Level 1(L1)	An Extended Fabric license is required. Extended Fabric port which can support up to 50 km at both 1 G and 2 G. This mode does not support trunking with other ports.
Level 2(L2)	An Extended Fabric license is required. Extended Fabric port which can support up to 100 km at 1 G and up to 60 km at 2 G. This mode does not support trunking with other ports.
Level 0.5 (L0.5)	Supports up to 25 km at both 1 G and 2 G. This mode was created to support 2 G up to 10 km and uses EF principles. This mode does not support trunking with other ports.
(Lx)	Any of L1, L2, LE, L0.5, and LD.

Level D (LD) (Dynamic long distance configuration)	LD mode dynamically assigns buffers based on the link round trip timing calculation. Ports are disabled when the buffer pool is depleted. For example, if two ports are configured at LD and each is connected at 100 km, all buffers are utilized and the remaining two ports are disabled. This mode supports up to 50 km at 1 G and 60 km at 2 G.

3. Repeat step 2 for the remote long distance ISL port. Both the local and remote long distance ISL ports must be configured to the same distance level for the connection to work. When the connection is initiated, the fabric is reconfigured.

VC Translation Mode

Revisions of Fabric OS v3.0.2 and later contain an additional optional parameter, VC Translation Link Initialization, to the `portCfgLongDistance` CLI command. When set to `1`, this parameter indicates that enhanced link reset protocol should be used on the port. The default value for this parameter is `0` and is compatible with earlier Fabric OS v3.x implementations.

For optimal performance, specify `1` when E_Port links are between switches with Fabric OS v3.0.2 and greater, or Fabric OS v4.0.2 and greater. Specify `0`, or nothing, when connecting a switch with Fabric OS v3.0.2 or above switch to previous releases of Fabric OS.

Distributed Fabric Commands

Table 12 lists commands that configure and manage the Extended Fabric or Remote Switch features.

Table 12: Distributed Fabric Commands

Command	Description
`configure`	This command is used for the Remote Switch feature. Use it to modify parameters necessary to ensure compatibility with the chosen gateway device. Note that v4.2.x does not support the extended link with HP StorageWorks 1 GB switches. The Long Distance fabric parameter is used to enable 1 GB switches to configure extended links with other switches.
`portcfglongdistance`	Configure a port to support a long distance ISL link. This command must be executed on both the ports used in a Long Distance ISL link.

For more information on these commands, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

The SAN Management Application

7

This chapter provides information on working with the Management Server (MS) platform database, and discusses the following major topics:

The Management Server

The Fabric Operating System (Fabric OS) includes a Distributed Management Server. The Management Server allows a Storage Area Network (SAN) management application to retrieve information and to administer the fabric and interconnected elements, such as switches, servers, and storage devices. The MS is located at the Fibre Channel well-known address, `FFFFFAh`.

The implementation of the Management Server (MS) provides four management services:

- Fabric Configuration Service - Provides basic configuration management for topology information (referred to as *Topology Discovery*).
- Unzoned Name Server access - Provides a management view of the Name Server information for all devices in a fabric, regardless of the active zone set.
- Fabric Zone Service
- FDMI

The services provided by the MS assist in the auto-discovery of switch-based fabrics and their associated topology. A client of the MS can determine basic information regarding the switches that comprise the fabric and use this information to construct topology relationships. In addition, the basic configuration services provided by the management server allow certain attributes associated with switches to be obtained, and in some cases, modified. For example, logical names identifying switches may be registered with the Management Server.

Note: The `msconfigure` command is disabled if the switch is in secure mode. Refer to the *HP StorageWorks Secure Fabric OS 4.2.x User Guide* for more information.

The MS allows for the discovery of the physical and logical topology that comprises a Fibre Channel SAN. The MS provides several advantages for managing a Fibre Channel fabric:

- It is accessed by an external Fibre Channel node at the well-known address `xFFFFFA`.
- It is replicated on every HP StorageWorks switch within a fabric (for Fabric OS v2.3 and later).
- It provides an unzoned view of the overall fabric configuration.

Because the MS is accessed via its well-known address, an application can access the entire fabric management information with minimal knowledge of the existing configuration. The fabric topology view exposes the internal configuration of a fabric for management purposes; it contains interconnect information about switches and devices connected to the fabric. Under normal circumstances, a device (typically an FCP initiator) queries the Name Server for storage devices within its member zones. Because this limited view is not always sufficient, the MS provides the application with a list of the entire Name Server database.

Note: Management Server Platform service is available only with Fabric OS V2.3 and later. If the Management Server Platform service is started on a fabric with any switches with v2.2.x or earlier, the MS Platform Services are disabled (the command is rejected).

Configuring Access to the Management Server

An Access Control List (ACL) of WWN addresses determines which systems have access to the Management Server database. If the list is empty (default), the Management Server is accessible to all systems connected in-band to the Fabric. For a more secured access, you can specify WWNs in the ACL. These WWNs are usually associated with the management applications. If any WWNs are entered into the ACL, access to the Management Server is restricted only to those WWNs listed in the ACL.

Displaying the Access Control List

To display the Management Server ACL:

1. Log in to the switch as admin.
2. Issue the `msconfigure` command. The command becomes interactive.
3. At the `select` prompt, enter `1` to display the access list. A list of WWNs that have access to the Management Server is displayed.

Example

```
switch:admin> msconfigure

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 1

done ...
switch:admin>
```

Adding a WWN to the Access Control List

To add a WWN to the ACL:

1. Log in to the switch as admin.
2. Issue the `msconfigure` command. The command becomes interactive.
3. At the `select` prompt enter `2` to add a member based on its Port/Node WWN.
4. At the prompt enter the WWN of the member you would like to add to the ACL.
5. Press **Enter**. The main menu displays.
6. At the prompt enter `1` to verify the WWN you entered was added to the ACL.
7. After you have verified that the WWN was added correctly, enter `0` at the prompt to end the session.
8. At the `Update the FLASH?` prompt enter `Y`.
9. Press **Enter** to update the flash and end the session.

Example

```
switch:admin> msconfigure

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 2

Port/Node WWN (in hex): [20:00:00:20:37:65:ce:aa]
*WWN is successfully added to the MS ACL.

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [2] 1

MS Access List consists of (14): {
 20:00:00:20:37:65:ce:aa
 20:00:00:20:37:65:ce:bb
 20:00:00:20:37:65:ce:ff
 20:00:00:20:37:65:ce:11
 20:00:00:20:37:65:ce:22
 20:00:00:20:37:65:ce:33
 20:00:00:20:37:65:ce:44
 10:00:00:60:69:04:11:24
 10:00:00:60:69:04:11:23
 21:00:00:e0:8b:04:70:3b
 10:00:00:60:69:04:11:33
 20:00:00:20:37:65:ce:55
 20:00:00:20:37:65:ce:66
 00:00:00:00:00:00:00:00
}


0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 0

done ...
Update the FLASH?  (yes, y, no, n): [yes] y
*Successfully saved the MS ACL to the flash.

switch:admin>
```

Deleting a WWN from the Access Control List

To delete a WWN from the ACL:

1. Log in to the switch as admin.
2. Issue the `msconfigure` command. The command becomes interactive.
3. At the `select` prompt enter `3` to delete a member based on its Port/Node WWN.
4. At the prompt enter the WWN of the member you would like to delete from the ACL.
5. Press **Enter**. The main menu is displayed.
6. At the prompt enter `1` to verify the WWN you entered was deleted from the ACL.
7. Once you have verified that the WWN was deleted correctly, enter `0` at the prompt to end the session.
8. At the `Update the FLASH?` prompt enter `Y`.
9. Press **Enter** to update the flash and end the session.

Example

```
switch:admin> msconfigure

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 3

Port/Node WWN (in hex): [20:00:00:20:37:65:ce:44]
*WWN is successfully deleted from the MS ACL.

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [2] 1

MS Access List consists of (13): {
 20:00:00:20:37:65:ce:aa
 20:00:00:20:37:65:ce:bb
 20:00:00:20:37:65:ce:ff
 20:00:00:20:37:65:ce:11
 20:00:00:20:37:65:ce:22
 20:00:00:20:37:65:ce:33
 10:00:00:60:69:04:11:24
 10:00:00:60:69:04:11:23
 21:00:00:e0:8b:04:70:3b
 10:00:00:60:69:04:11:33
 20:00:00:20:37:65:ce:55
 20:00:00:20:37:65:ce:66
}


0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 0

done ...
Update the FLASH?  (yes, y, no, n): [yes] y
*Successfully saved the MS ACL to the flash.

switch:admin>
```

Displaying the Management Server Database

To view the contents of the Management Server Platform Database:

1. Log in to the switch as admin.
2. Issue the `msplatshow` command. The contents of the Management Server Database are displayed.

Example

```
switch:admin> msplatshow
-----------------------------------------------------------
Platform Name: [9] "first obj"
Platform Type: 5 : GATEWAY
Number of Associated M.A.: 1
[35] "http://java.sun.com/products/plugin"
Number of Associated Node Names: 1
Associated Node Names:
10:00:00:60:69:20:15:71
-----------------------------------------------------------
Platform Name: [10] "second obj"
Platform Type: 7 : HOST_BUS_ADAPTER
Number of Associated M.A.: 1
Associated Management Addresses:
[30] "http://java.sun.com/products/1"
Number of Associated Node Names: 1
Associated Node Names:
10:00:00:60:69:20:15:75
```

Clearing the Management Server Database

To clear the MS Platform database:

1. Log in to the switch as admin.
2. Issue the `msplcleardb` command.
3. Enter `Y` to confirm the deletion. The Platform database is cleared.

Activating the Platform Management Service

To activate the Platform Management Service for a fabric:

1. Log in to the switch as admin.
2. Issue the `msplmgmtactivate` command.

Example

```
switch:admin> msplmgmtactivate

Activating Platform Management Service in the Fabric is in progress......

*Completed activating Platform Management Service in the fabric!

switch:admin>
```

Deactivating the Platform Management Service

To deactivate the Platform Management Service for a fabric:

1. Log in to the switch as admin.
2. Issue the `msplmgmtdeactivate` command.
3. Enter `Y` to confirm the deactivation.

Example

```
switch:admin> msplmgmtdeactivate

MS Platform Management Service is currently enabled.

This will erase Platform configuration information
as well as Platform databases in the entire fabric.

Would you like to continue disabling? (yes, y, no, n): [no] y

Deactivating Platform Management Service is in progress......

*Completed deactivating Platform Management Service in the
fabric!

switch:admin>
```

Controlling the Topology Discovery

Topology Discovery is a feature within the Management Server and can be displayed, enabled, and disabled separately.

Display Topology Discovery Status

To display the current status of this feature:

1. Log in to the switch as admin.
2. Issue the `mstdreadconfig` command.

Example

```
switch:admin> mstdreadconfig
*MS Topology Discovery is Enabled.
switch:admin>
```

Enabling the Topology Discovery Feature

The Topology Discovery feature is disabled by default. To enable the feature:

1. Log in to the switch as admin.
2. Issue the `mstdenable` command. A request is sent to enable the Topology Discovery feature and it is enabled.

Note: The ALL argument enables the feature on the whole fabric.

Example

```
switch:admin> mstdenable
Committing configuration...done.
switch:admin> mstdenable ALL
Committing configuration...done.
```

Disabling the Topology Discovery Feature

Caution: Disabling the Topology Discovery feature may erase all NID entries.

To disable the Topology Discovery feature:

1. Log in to the switch as admin.
2. At the command, line issue the `mstddisable` command. A warning displays, informing you that all NID entries may be cleared.
3. Enter `Y` to disable MS Topology discovery.

Example

```
switch:admin> mstddisable
This will erase all NID entries. Are you sure? (yes, y, no, n): [no] y
Committing configuration...done.
switch:admin> mstddisable ALL
This will erase all NID entries. Are you sure? (yes, y, no, n): [no] y
Committing configuration...done.
```

Performance Monitor Procedures

8

This chapter provides information on procedures for using the Performance Monitor feature using Fabric OS commands. This feature requires a license key to activate.

This chapter discusses the following major topics:

License Activation

Use the `licenseshow` command to verify that the *Performance Monitor* license key is installed to your switch. See "Managing Licensed Features" on page 39 for more information on activating a feature using license keys.

Performance Monitor Commands

Table 13 lists commands used to configure and manage the Performance Monitor feature. For detailed information on these commands, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

Table 13: Performance Monitor Commands

Command	Description
`perfaddeemonitor`	Add an end-to-end monitor to a port
`perfaddipmonitor`	Add an IP monitor to a port
`perfaddreadmonitor`	Add a SCSI Read monitor to a port
`perfaddrwmonitor`	Add a SCSI Read and Write monitor to a port
`perfaddscsimonitor`	Add a SCSI traffic frame monitor to a port
`perfaddusermonitor`	Add a user-defined monitor to a port
`perfaddwritemonitor`	Add a SCSI Write monitor to a port.
`perfcfgclear`	Clear the performance monitoring settings from flash memory
`perfcfgrestore`	Restore performance monitoring settings from flash memory
`perfcfgsave`	Save the current performance monitoring settings to flash memory.
`perfcleareemonitor`	Clear statistics counters of an end-to-end monitor on a port
`perfclearfiltermonitor`	Clear statistics counters of a filter-based monitor
`perfclralpacrc`	Clear an ALPA device CRC count by the port and by ALPA
`perfdeleemonitor`	Delete an end-to-end monitor on a port
`perfdelfiltermonitor`	Delete a filter-based monitor
`perfsetporteemask`	Set overall mask for end-to-end (EE) monitors.
`perfshowalpacrc`	Display the ALPA CRC count by port or by ALPA.
`perfshoweemonitor`	Display user-defined end-to-end monitors on a port
`perfshowfiltermonitor`	Display filter-based monitors on a port
`perfshowporteemask`	Display the current end-to-end mask of a port

AL_PA Performance Monitoring

AL_PA performance monitoring tracks and displays the number of CRC errors that have occurred on frames sent from each AL_PA on a specific port. AL_PA-based performance monitoring does not require explicit configuration. The switch hardware and firmware automatically monitor CRC errors for all valid AL_PAs.

Note: On a system with a blade, the `slot/port` syntax is used. On a system without blades, the port number is used. All examples in this document use slot/port syntax.

Displaying the CRC Error Count

To display the CRC error count for all AL_PA devices or for a single AL_PA on a specific port, use the `perfshowalpacrc` command. The port must be an active L_Port. The command used in the example displays the CRC error count for all AL_PA devices on port 3 (on slot 1).

Example

```
switch:admin> perfshowalpacrc 1/3
AL_PA    CRC count
--------------------
0x01     2
0x02     0
0x04     1
```

The command used in the following example displays the CRC error count for AL_PA 0x01 on slot 1 port 3.

Example

```
switch:admin> perfshowalpacrc 1/3, 0x01
The CRC count at ALPA 0x1 on port 3 is 0x000000002.
```

Clearing the CRC Error Count

To clear the CRC error count for AL_PA devices on a specific port, use the `perfclralpacrc` command. Using this command you can either clear the error counts for a specific AL_PA or clear the error counts on all AL_PA devices

on a port. The command used in the first example below clears the CRC error count for all AL_PA devices on slot 1 port 3. The command used in the second example below clears the CRC error count for AL_PA 0x01 on slot 1 port 3.

Note: In v3.1 and v4.2 issuing the `portstatsclear` command on a port also results in all AL_PA-based CRC error counters being cleared for all ports in the same quad.

Example

```
switch:admin> perfclralpacrc 1/3
No ALPA value is specified. This will clear all ALPA CRC
counts on port 3. Do you want to continue? (yes, y, no, n): [no]
Please wait ...
All alpa CRC counts are cleared on port 3.
```

Example

```
switch:admin> perfclralpacrc 1/3, 0x01
CRC error count at ALPA 0x1 on port 3 is cleared.
```

End-to-End Performance Monitoring

End-to-end performance monitoring counts the number of words and CRC errors in Fibre Channel frames for a specified Source ID (SID) and Destination ID (DID) pair. An end-to-end performance monitor counts the number of:

- Words in frames received at the port (RX_COUNT).
- Words in frames transmitted from the port (TX_COUNT).
- Frames received at or transmitted from the port with CRC errors (CRC_COUNT).

To enable end-to-end performance monitoring, you must configure an end-to-end monitor on a port, specifying the SID-DID pair. The monitor counts only those frames with matching SID and DID.

Each SID or DID has three fields, listed in the following order:

- Domain ID (DD)
- Area ID (AA)
- AL_PA (PP)

The SID 0x118a0f has Domain ID 0x11, Area ID 0x8a, and AL_PA 0x0f. The prefix “0x” denotes a hexadecimal number.

Adding End-to-End Monitors

Use this command to add an end-to-end monitor to a port. The monitor counts the number of words received, number of words transmitted, and number of CRC errors detected in frames qualified, using either of following two conditions:

1. For frames received at the port (with end-to-end monitor installed), the frame SID is the same as the SourceID and the frame DID is the same as the DestID. Both RX_COUNT and CRC_COUNT are updated accordingly.
2. For frames transmitted from the port (with end-to-end monitor installed), the frame DID is the same as the SourceID and the frame SID is the same as the DestID. TX_COUNT, and CRC_COUNT are updated accordingly.

Depending on the application, any port along the routing path can be selected for monitoring.

Note: How the area ID for a port relates to the port number depends upon the PID format used by the fabric. See Chapter 13, “Selecting a Switch PID Format,” for more information.

Figure 4 shows two devices to be monitored:

- Host A, which is connected to domain 5 (0x05), switch area ID 18 (0x12), AL_PA 0x00 on Switch X
- Dev B, which is connected to domain 17 (0x11), switch area ID 30 (0x1e), AL_PA 0xef on Switch Y.

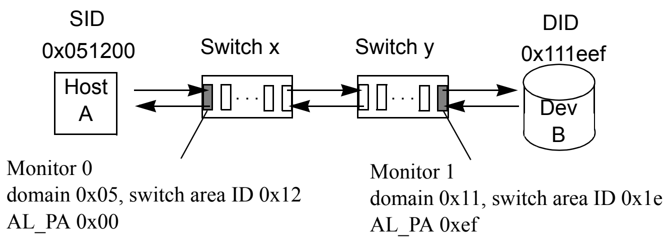

Figure 4: Setting End-to-End Monitors on a Port

- To monitor the traffic from Host A to Dev B, add a monitor to slot 1, port 2, specifying `0x051200` as the SID and `0x111eef` as the DID.
- To monitor the traffic from Dev B to Host A, add a monitor to slot 2, port 15, specifying `0x111eef` as the SID and `0x051200` as the DID. Use the commands shown in the two examples below.

Example

```
switch:admin> perfaddeemonitor 1/12, "0x051200" "0x111eef"
End-to-End monitor number 0 added.
```

Example

```
switch:admin> perfaddeemonitor 2/14, "0x111eef" "0x051200"
End-to-End monitor number 1 added.
```

- Monitor 0 counts the frames that have an SID of `0x051200` and a DID of `0x111eef`. For monitor 0, RX_COUNT is the number of words from Host A to Dev B, TX_COUNT is the number of words from Dev B to Host A, and CRC_COUNT is the number of frames in both directions with CRC errors.
- Monitor 1 counts the frames that have an SID of `0x111eef` and a DID of `0x051200`. For monitor 1, RX_COUNT is the number of words from Dev B to Host A, TX_COUNT is the number of words from Host A to Dev B, and CRC_COUNT is the number of frames in both directions with CRC errors.

Note: End-to-end performance monitoring monitors traffic on the receiving port only for the SID. In Figure 4, if you add a monitor to slot 2, port 14, specifying Dev B as the SID and Host A as the DID, only the CRC counter is incremented.

Figure 5 shows several switches and the proper ports on which to add performance monitors for a specified SID-DID pair.

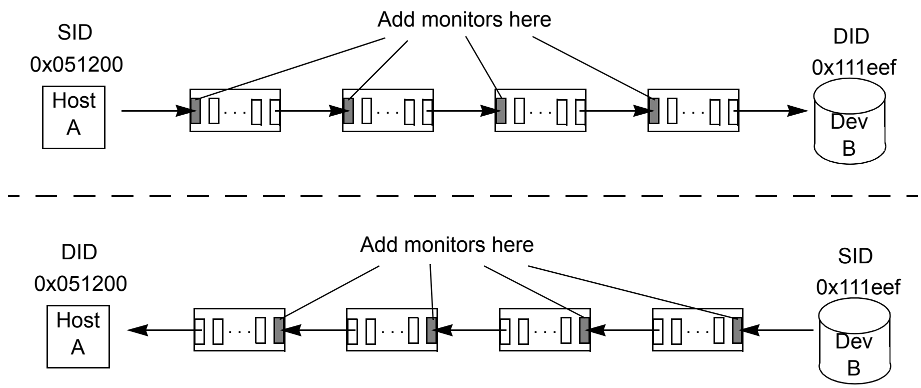

Figure 5: Proper Placement of End-to-End Performance Monitors

Setting a Mask for End-to-End Monitors

End-to-end monitors count the number of words in Fibre Channel frames that match a specific SID/DID pair. If you want to match only part of the SID or DID, you can set a mask on the port to compare only certain parts of the SID or DID. With no mask set, the frame must match the entire SID and DID to trigger the monitor. By setting a mask, you can choose to have the frame match only one or two of the three fields (Domain ID, Area ID, AL_PA) to trigger the monitor.

Only one mask per port can be set. When setting a mask, all existing end-to-end monitors are deleted. The following example specifies the mask in the form.

Example

```
"dd:aa:pp"
```

where:

- *dd* is the Domain ID mask
- *aa* is the Area ID mask
- *pp* is the AL_PA mask.

The values for *dd*, *aa*, and *pp* are either `ff` (the field must match) or `00` (the field is ignored).

To set a mask for end-to-end monitors, issue the `perfsetporteemask` command. The command sets the mask for all end-to-end monitors of a port.

If any end-to-end monitors are programmed on a port when the `perfsetporteemask` command is issued, you see the message displayed as in the following example.

Example

```
'< n > EE monitors are currently programmed on this port. Changing EE mask
for this port will cause ALL EE monitors on this port to be deleted.
Do you want to continue? (yes, y, no, n): [no]

EE mask on port <port-number> is set and EE monitors were deleted
```

The `perfsetporteemask` command sets a mask for the Domain ID, Area ID, and AL_PA of the SIDs and DIDs for frames transmitted from and received by the port. Figure 6 shows the mask positions in the command.

In Figure 6, a mask (`ff`) is set on slot 1, port 2 to compare the AL_PA fields on the SID and DID in all frames (transmitted and received) on port 2. The frame SID and DID must match only the AL_PA portion of the specified SID-DID pair. Each port can have only one EE mask. The mask is applied to all end-to-end monitors on the port. Individual masks for each monitor on the port cannot be specified. The default EE mask value upon power-on is ff:ff:ff for everything—SID and DID on all transmitted and received frames. on the port. Individual masks for each monitor on the port cannot be specified.

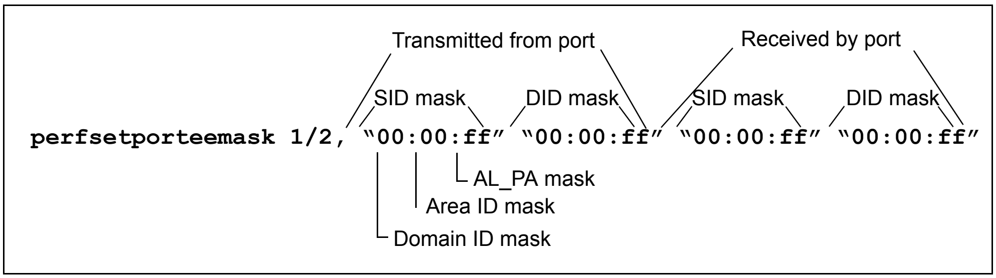

Figure 6: Mask Positions for End-to-End Monitors

Example

```
perfaddeemonitor 1/2, "0x051200" "0x111eef"
```

If the monitor on a port is set as in the example, then the frame SID must be `0x051200`, and the frame DID must be `0x111eef` to trigger the monitor.

Displaying the End-to-End Mask of a Port

The `perfshowporteemask` command is used to display the current end-to-end mask of a port. The end-to-end mask has 12 fields, and each field has a value of `on` or `off`. The examples sets an end-to-end mask on slot 1, port 11 and displays the mask.

Example

```
switch:admin> perfsetporteemask 1/11,
"00:00:ff" "00:00:ff" "00:00:ff" "00:00:ff"
The EE mask on port 11 is set and EE counters are reset.
```

Example

```
switch:admin> perfshowporteemask 1/11
The EE mask on port 11 is set by application TELNET
TxSID Domain:  off
TxSID Area:    off
TxSID ALPA:    on
TxDID Domain:  off
TxDID Area:    off
TxDID ALPA:    on
RxSID Domain:  off
RxSID Area:    off
RxSID ALPA:    on
RxDID Domain:  off
RxDID Area:    off
RxDID ALPA:    on
```

Displaying End-to-End Monitors

The `perfshoweemonitor` command is used to display all the end-to-end monitors defined on a port. Cumulative counters, or a rolling table of counters, can be displayed at specified intervals.

This command displays the following information on all end-to-end monitors:

- Monitor number (KEY)
- SID
- DID
- CRC error count (CRC_COUNT)
- Number of Fibre Channel words transmitted (TX_COUNT)
- Number of Fibre Channel words received (RX_COUNT)
- Creator application (OWNER_APP)
- IP address of the creator, if known (OWNER_IP_ADDR)

If an interval number is specified in the `perfshoweemonitor` command, the command displays a rolling table of CRC errors, TX counters, and RX counters on a per-interval basis for all the valid monitors on the port. The counter values are the number of bytes, in decimal format.

If you omit the display interval number, the command displays the cumulative transmit counter (TX_COUNT), receive counter (RX_COUNT), and CRC error counter. These cumulative counters are 64-bit values in hexadecimal format.

The following example displays all of the end-to-end monitors on slot 1, port 3. In this example, three monitors are on slot 1, port 3. The monitors are numbered 0, 1, and 2.

Note: In v4.x, registers are scanned every 5 seconds and display intervals should be specified in multiples of 5 seconds. In v3.x, there is no requirement for the interval restriction.

Example

```
switch:admin> perfshoweemonitor 1/3, 5
perfShowEEMonitor 3, 5: Tx/Rx are # of bytes and crc is # of crc errors

     0             1             2
------------  ------------  ------------
crc   Tx   Rx  crc   Tx   Rx  crc   Tx   Rx
============  ============  ============
 0    0     0    0    0     0    0    0     0
 0   53m  4.9m   0   53m  4.9m   0   53m  4.9m
 0   53m  4.4m   0   53m  4.4m   0   53m  4.4m
 0   53m  4.8m   0   53m  4.8m   0   53m  4.8m
 0   53m  4.6m   0   53m  4.6m   0   53m  4.6m
 0   53m  5.0m   0   53m  5.0m   0   53m  5.0m
 0   52m  4.6m   0   52m  4.6m   0   52m  4.6m
```

Note: In the above example, `m` means *megabytes*. You may also see `g` for gigabytes, or `k` for kilobytes.

The example displays the cumulative counters on all end-to-end monitors defined on slot 1, port 3. The KEY column contains the monitor number.

Example

```
switch:admin> perfshoweemonitor 1/3
There are 3 end-to-end monitor(s) defined on port 3.
KEY  SID      DID    OWNER_APP  OWNER_IP_ADDR    TX_COUNT           RX_COUNT            CRC_COUNT
----------------------------------------------------------------------------------------------------
-
0 0xb1300  0xb23ef   TELNET        NA     0x00000004d0ba9915  0x0000000067229e65  0x0000000000000000
1 0xb1200  0xb22ef   TELNET        NA     0x00000004d0baa754  0x0000000067229e87  0x0000000000000000
2 0x58e0f  0x1182ef WEB_TOOLS 192.168.169.40 0x00000004d0bade54 0x0000000067229e87 0x000000000000000
0
```

Deleting End-to-End Monitors

The perfdeleemonitor command is used to delete an end-to-end monitor on a port. Indicate which monitor to delete by specifying the monitor number that was returned by a previous perfaddeemonitor command. The example deletes the end-to-end monitor number 0 on slot 1, port 2.

Example

```
switch:admin> perfdeleemonitor 1/2, 0
End-to-End monitor number 0 deleted
```

Clearing End-to-End Monitor Counters

To clear statistics counters for one or all end-to-end monitor on a port, use the perfcleareemonitor command. After the command has been executed, the Telnet shell confirms that the monitor counters have been cleared.

Before issuing this command, verify that all of the valid end-to-end monitor numbers on a specific port issue the perfshoweemonitor command to clear the correct monitor counters. The example below clears statistic counters for an end-to-end monitor on slot 1, port 2, monitor 5.

Note: In v4.2 and v3.1 issuing the command portstatsclear on a port also results in all End-to-End monitors being cleared for all the ports in the same quad.

Example

```
switch:admin> perfcleareemonitor 1/2, 5
End-to-End monitor number 5 counters are cleared
```

Filter-based Performance Monitoring

Filter-based monitoring counts the number of times a frame with a particular pattern is received by a port. To use filter-based monitoring, you configure a specific filter for a particular purpose. The filter can be a standard filter (for example, a read command filter that counts the number of read commands that have been received by the port) or a user-defined filter that you customize for your particular use.

The maximum number of filters is eight per port, in any combination of standard filters and user-defined filters. The actual number of filters that can be configured on a port depends on the complexity of the filters.

Adding Standard Filter-based Monitors

Table 14 lists the Telnet commands used when you add standard filter-based monitors to a port.

Table 14: Telnet Commands to Add Filter-Based Monitors

Telnet Command	Description
`perfaddreadmonitor`	Count the number of SCSI Read commands
`perfaddwritemonitor`	Count the number of SCSI Write commands
`perfaddrwmonitor`	Count the number of SCSI Read and Write commands
`perfaddscsimonitor`	Count the number of SCSI traffic frames
`perfaddipmonitor`	Count the number of IP traffic frames

The example adds filter-based monitors to port 2 using the `perfaddreadmonitor` command and displays the results.

Example

```
switch:admin> perfaddreadmonitor 1/2
SCSI Read filter monitor #0 added
```

The following example adds filter-based monitors to port 2 using the `perfaddwritemonitor` command and displays the results.

Example

```
switch:admin> perfaddwritemonitor 1/2
SCSI Write filter monitor #1 added
```

The following example adds filter-based monitors to port 2 using the `perfaddrwmonitor` command and displays the results.

Example

```
switch:admin> perfaddrwmonitor 1/2
SCSI Read/Write filter monitor #2 added
```

The following example adds filter-based monitors to port 2 using the `perfaddscsimonitor` command and displays the results.

Example

```
switch:admin> perfaddscsimonitor 1/2
SCSI traffic frame monitor #3 added
```

The following example adds filter-based monitors to port 2 using the `perfaddipmonitor` command and displays the results.

Example

```
switch:admin> perfaddipmonitor 1/2
IP traffic frame monitor #4 added
```

The following example displays filter-based monitors configured on port 2 using the `perfshowfiltermonitor` command.

Example

```
switch:admin> perfshowfiltermonitor 1/2
There are 5 filter-based monitors defined on port 2.

KEY   ALIAS   OWNER_APP       OWNER_IP_ADDR     FRAME_COUNT
----------------------------------------------------------------
0  SCSI Read  TELNET                 N/A       0x0000000000000000
1  SCSI Write TELNET                 N/A       0x0000000000000000
2  SCSI R/W   TELNET                 N/A       0x0000000000000000
3  SCSI Frame TELNET                 N/A       0x0000000000000000
4  IP Frame   TELNET                  N/A       0x0000000000000000
```

Adding User-defined Filter-based Monitors

In addition to the standard filters (read, write, read/write, and frame count), you can create custom filters to qualify frames to gather statistics to fit your needs.

To define a custom filter, use the `perfaddusermonitor` Telnet command. With this command, you must specify a series of offsets, masks, and values.

For all incoming frames, the switch:

- Locates the byte found in the frame at the specified offset.
- Applies the mask to the byte found in the frame.
- Compares the value with the given values in the `perfaddusermonitor` command.
- Increments the filter counter if a match is found.

Up to six different offsets for each port and up to four values to compare against each offset can be specified. If more than one offset is required to properly define a filter, the bytes found at each offset must match one of the given values for the filter to increment its counter. If one or more of the given offsets does not match any of the given values, the counter does not increment.

The value of the offset must be between 0 and 63, in decimal format. Byte 0 indicates the first byte of the Start of Frame (SOF), byte 4 is the first byte of the frame header, and byte 28 is the first byte of the payload. Thus, only the SOF, frame header, and first 36 bytes of payload may be selected as part of a filter definition. Offset 0 is a special case, which can be used to monitor the first 4 bytes of the frame (SOF). When the offset is 0, the values are from 0–7, as indicated in Table 15.

Table 15: Offset and SOF Values

Offset	SOF Value
0	SOFf
1	SOFc1
2	SOFi1
3	SOFn1
4	SOFi2
5	SOFn2
6	SOFi3
7	SOFn3

The hardware can manage only 16 unique offsets and values per port, 13 of which are already specified. This leaves three offsets that can be used for new user defined offsets. If the switch does not have enough resources to create a given filter, then other filters might have to be deleted to free up resources.

The following example adds a filter-based monitor to count all FCP and IP frames received from domain 0x02 for port 2 on slot 4. The FCP and IP protocols are selected by monitoring offset 12, mask 0xff and matching values of 0x05 or 0x08. Domain 2 is selected by monitoring offset 9, mask 0xff, and matching a value of 0x02.

Example

```
switch:admin> perfaddusermonitor 4/2,
"12, 0xff, 0x05, 0x08; 9, 0xff, 0x02" "FCP/IP"
User monitor #5 added
```

The monitor counter is incremented for all outgoing frames from port 2 where byte 9 is 0x02 and byte 12 is 0x05 or 0x08.

The following example adds a special case filter-based monitor for SOFi3 on slot 1, port 2.

Example.

```
switch:admin> perfaddusermonitor 1/2, "0, 0xff, 6"
User Monitor #6 added
```

Displaying Filter-based Monitors

Use the `perfshowfiltermonitor` command to display all the filter-based monitors on a specified port. The cumulative count of the traffic detected by the monitors can be displayed, or you can display a snapshot of the traffic at specified intervals.

Note: In v4.x, registers are scanned every 5 seconds and display intervals should be specified in multiples of 5 seconds. In v3.x, there is no requirement for the interval restriction.

The following example displays filter monitor traffic on slot 1, port 2 at an interval of once every 5 seconds. In the command output, `#CMDs` refers to the read, write, and read-write counters, and `#Frames` refers to SCSI frame, IP frame, and user-defined counters.

Example.

```
switch:admin> perfshowfiltermonitor 1/2, 5
    0        1        2        3        4        5        6
  #CMDs    #CMDs    #CMDs   #Frames  #Frames  #Frames   #CMDs
-------------------------------------------------------------
    0         0        0        0        0        0        0
   26k      187      681      682      682      494      187
   26k      177      711      710      710      534      176
   26k      184      734      734      734      550      184
   26k      182      649      649      649      467      182
   26k      188      754      755      755       567       184
```

The following example displays the cumulative frame count of all filter-based monitors defined on slot 1, port 2. The KEY column lists the monitor numbers.

Example

```
switch:admin> perfshowfiltermonitor 1/2
There are 7 filter-based monitors defined on port 2.
KEY   ALIAS   OWNER_APP       OWNER_IP_ADDR     FRAME_COUNT
----------------------------------------------------------------
0  SCSI Read  TELNET                N/A       0x0000000000002208
1  SCSI Write TELNET                N/A       0x000000000000464a
2  SCSI R/W   TELNET                N/A       0x000000000000fd8c
3  SCSI Frame WEB_TOOLS       192.168.169.40 0x00000000002c2229
4  IP Frame   WEB_TOOLS       192.168.169.40 0x0000000000000492
5  FCP/IP     WEB_TOOLS       192.168.169.40 0x0000000000000009
6  SCSI_RD    WEB_TOOLS      192.168.161.140 0x000000000000023a
```

Deleting Filter-based Monitors

To delete a filter-based monitor:

1. List the valid monitor numbers using the `perfshowfiltermonitor` command.
2. Use the `perfdelfiltermonitor` command to delete a specific monitor. If you do not specify which monitor number to delete, you are asked if you want to delete all entries.

The following example displays the monitors on slot 1, port 4 using the `perfshowfiltermonitor` command (the monitor numbers are listed in the KEY column).

Example

```
switch:admin> perfshowfiltermonitor 1/4
There are 4 filter-based monitors defined on port 4.
KEY   ALIAS   OWNER_APP       OWNER_IP_ADDR     FRAME_COUNT
------------------------------------------------------------------
0   SCSI Read  TELNET                 N/A       0x0000000000002208
1   SCSI Write TELNET                 N/A       0x000000000000464a
2   SCSI R/W   TELNET                 N/A       0x000000000000fd8c
3   SCSI Frame WEB_TOOLS       192.168.169.40 0x00000000002c2229
```

The following example deletes monitor number 1 on slot 1, port 4 using the `perfdelfiltermonitor` command.

Example

```
switch:admin> perfdelfiltermonitor 1/4, 1
The specified filter-based monitor is deleted.
```

Clearing Filter-based Monitor Counters

Before you clear statistics counters, verify all of the valid monitor numbers with user-defined aliases on a specific port using the `perfshowfiltermonitor` command, to make sure the correct monitor counters are cleared. To clear statistics counters for all filter-based monitors or for a specific one, use the `perfclearfiltermonitor` command. After the command has been executed, the Telnet shell confirms that the counters on the monitor have been cleared.

Note: In v4.2 and v3.1 issuing the command `portStatsClear` on a port also results in all filter-based monitors being cleared for all the ports in the same quad.

The following example clears the statistics counters for a filter-based monitor 4 on port 2 in slot 1.

Example

```
switch:admin> perfclearfiltermonitor 1/2, 4
Filter-based monitor number 4 counters are cleared
```

Saving and Restoring Monitor Configurations

The `perfcfgsave` commands used to save the current end-to-end and filter-based monitor configuration settings into flash memory. You can use the `perfcfgrestore` command to restore the saved monitor configuration from flash memory. For example, after a power cycle you should use the same end-to-end and filter-based monitor configuration that was in effect before the power cycle.

To save a filter-based monitor configuration use the `perfcfgsave` command.

Example

```
switch:admin> perfcfgsave
This will overwrite previously saved Performance Monitoring settings in FLASH ROM. Do
you want to continue? (yes, y, no, n): [no]
Please wait...
Committing configuration...done.
Performance monitoring configuration saved in FLASH ROM.
```

To restore a filter-based monitor configuration use the `perfcfgrestore` command to restore the saved monitor configuration.

Example

```
switch:admin> perfcfgrestore
This will overwrite current Performance Monitoring settings in RAM. Do you
want to continue? (yes, y, no, n): [no]
Please wait...
Performance monitoring configuration restored from FLASH ROM.
```

You can use the `perfcfgclear` command to clear the previously saved performance monitoring configuration settings from flash memory, as in the following example.

Example

```
switch:admin> perfcfgclear
This will clear Performance Monitoring settings in FLASH ROM. The RAM
settings won't change.  Do you want to continue? (yes, y, no, n): [no]
Please wait...
Committing configuration...done.
Performance Monitoring configuration cleared from FLASH.
```

ISL Trunking Procedures

9

This chapter provides information on procedures for using the ISL Trunking feature using Fabric OS commands. This feature requires a license key to activate.

This chapter discusses the following major topics:

License Activation

Use the `licenseshow` command to verify that the Trunking license key is installed to your switch. See “Managing Licensed Features” on page 39 for more information on activating a feature using license keys.

ISL Trunking Commands

Table 16 lists commands that configure and manage ISL Trunking. For detailed information on these commands, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

Table 16: ISL Trunking Commands

Command	Use
`portcfgspeed`	Specify the port speed
`portcfgtrunkport`	Enable or disable trunking for a port
`portperfshow`	Monitor traffic across ports, so that you can optimize trunking in your fabric
`switchcfgspeed`	Set all ports of the switch to a particular speed
`switchcfgtrunk`	Enable or disable trunking for all the ports of a switch
`trunkdebug`	Debug a trunk link failure
`trunkshow`	Display trunking information

Gathering Traffic Data

HP recommends that you monitor your traffic to determine the optimal location in your fabric to implement trunking.

Using the CLI to View Traffic Data

The `portperfshow` command can be used to record the traffic volume for each port over time to identify the congested paths that would benefit from the implementation of trunking groups. This command can also be used to identify frequently dropped links, so that troubleshooting can be performed and the links can be added back to trunking groups as necessary.

To gather traffic data:

1. Log in to the switch as admin.
2. Issue the following command:

   `portperfshow [interval]`

   where *interval* is the number of seconds between each sample. If no interval is specified, the frequency defaults to one sample every 1 second.
3. Record the traffic flow for each port that is participating in an ISL.
4. Repeat step 1 through step 5 for the other switches in the fabric as required, until all ISL traffic flow is captured (in a very large fabric, it may be necessary to identify and capture the key ISLs only).
5. Repeat step 1 through step 3 throughout the day (or entire work cycle) to capture varying traffic patterns.

   Example

   The following example for an HP StorageWorks SAN Switch 2/8-EL with no trunking shows under-utilized links (ports 0, 1, 2) and congested links (ports 4, 5).

```
switch:admin> portperfshow
0      1      2      3      4      5      6      7      Total
-----------------------------------------------------------------
--
0      0      0      145m   204m   202m   0      168m   719
0      0      0      145m   206m   208m   0      186m   745
switch:admin>
```

Example

The following example shows traffic flowing through a trunking group of three ports, with one of the links failing after the second reading. This causes redistribution of traffic over the remaining two links in the group.

```
switch:admin> portperfshow
0      1      2      3      4      5      6      7      Total
------------------------------------------------------------
-
0      0      0      0      0      145m   144m   145m   434
0      0      0      0      0      144m   143m   144m   431
0      0      0      0      0      162m   0      162m   324
0      0      0      0      0      186m   0      186m   372
0      0      0      0      0      193m   0      192m   385
0      0      0      0      0      202m   0      202m   404
0      0      0      0      0      209m   0      209m   418
switch:admin>
```

Using Performance Monitoring to View Traffic Data

Performance Monitoring can be used to monitor traffic flow and to view the impact of different fabric configurations on performance.

For instructions on using Performance Monitoring, see Chapter 8, “Performance Monitor Procedures” on page 175.

Using Fabric Watch to Gather Traffic Data

Fabric Watch can be used to monitor traffic flow through specified ports on the switch and send alerts when the traffic exceeds or drops below configurable thresholds. This lets you monitor changes in traffic patterns and adjust the fabric design accordingly, such as by adding, removing, or reconfiguring ISLs and trunking groups.

For instructions on configuring Fabric Watch thresholds and alerts, refer to the *HP StorageWorks Fabric Watch 4.2.x User Guide*.

Enabling and Disabling ISL Trunking

Trunking can be enabled and disabled for an individual port or an entire switch. This is discussed in the following sections.

Enabling and Disabling Trunking on a Port

Telnet and serial sessions can be used to enable and disable trunking.

To enable or disable trunking for an individual port:

1. Log in to the switch as admin.
2. Enter the following command:

   `portcfgtrunkport` *`slotnumber/portnumber`* `1|0`

   where:

`slotnumber`	Specifies number of slot in which the port card containing the port is located; required only for switches with slots.
`portnumber`	Specifies port number on which to enable or disable trunking.
`1|0`	Enables or disables trunking; specify `1` to enable this port for trunking, or `0` to disable this port for trunking.

   Example

   To enable trunking for slot 1 port 3:

```
switch:admin> portcfgtrunkport 1/3 1
done.
switch:admin>
```

Enabling and Disabling Trunking for All Ports on a Switch

To enable or disable trunking for ALL the ports on a switch:

1. Log in to the switch as admin.
2. Enter the following command:

   `switchcfgtrunk 1|0`

   Specify `1` to enable trunking on all ports in the switch, or `0` to disable trunking on all ports in the switch.

Example

To enable all ports on the switch for trunking:

```
switch:admin> switchcfgtrunk 1
Committing configuration...done.
switch:admin>
```

Setting Port Speed

Port speeds can be set for the entire switch or for individual ports. If trunking is enabled, the only supported speeds are 2 Gbit/sec and auto-negotiate. If trunking is not enabled, 1 Gbit/sec is also supported.

Setting the Speed for All Ports on a Switch

To specify the speed for all the ports on the switch:

1. Log in to the switch as admin.
2. Enter the following command:

   `switchcfgspeed` *`speedlevel`*

   `Speedlevel` Link speed, as follows:

   `0` Auto-negotiating mode. The port automatically configures for the highest speed.

   `1` 1 Gbit/sec mode. The port is at a fixed speed of 1 Gbit/sec. This setting is not supported if trunking is enabled on the port.

   `2` 2 Gbit/sec mode. The port is at a fixed speed of 2 Gbit/sec.

Examples

To set the speed for all ports on the switch to 2 Gbit/sec:

```
switch:admin> switchcfgspeed 2
Committing configuration...done.
switch:admin>
```

To set the speed for all ports on the switch to auto-negotiate:

```
switch:admin> switchcfgspeed 0
Committing configuration...done.
switch:admin>
```

Setting the Speed for a Port

To specify the speed for an individual port:

1. Log in to the switch as admin.
2. Enter the following command:

   `portcfgspeed` *`slotnumber/portnumber speedlevel`*

`slotnumber`	Number of the switch slot; required only for switches with slots.
`portnumber`	Number of the port
`speedlevel`	Speed of the link, as follows: `0` Auto-negotiating mode; port automatically configures for highest speed `1` 1 Gbit/sec mode; fixes port at fixed speed of 1 Gbit/sec (not supported if trunking is enabled on the port) `2` 2 Gbit/sec mode; fixes port at fixed speed of 2 Gbit/sec

Examples

Setting the speed for port 3 on slot 2 to 2 Gbit/sec:

```
switch:admin> portcfgspeed 2/3 2
done.
switch:admin>
```

Setting the speed for port 3 on slot 2 to auto-negotiate:

```
switch:admin> portcfgspeed 2/3 0
done.
switch:admin>
```

Displaying Trunking Information

Web Tools or a Telnet or serial session can be used to view information about the trunking groups that exist on the local switch.

Displaying Trunking Information

The `trunkshow` command can be used to display information about trunking groups. This command provides information in the following columns:

- Column 1: number of the trunking group.
- Column 2: port-to-port connections of the group, listed by port number (local port -> remote port).
- Column 3: WWNs of the local ports in the group.
- Column 4: deskew values - the time difference for traffic to travel over each ISL as compared to the shortest ISL in the group. The number corresponds to nanoseconds divided by 10. The firmware automatically sets the minimum deskew value of the shortest ISL to 15.
- Column 5: specifies whether the port is the master port for the trunking group.

To display trunking information:

1. Log in to the switch as admin.
2. Enter the following command:

   `trunkshow`

   Example

   To display ISL Trunking information on a switch:

```
 switch:admin> trunkshow
 1: 1 ->  1   10:00:00:60:69:04:10:83   deskew 16 Master
    0 ->  0   10:00:00:60:69:04:10:83   deskew 15

 2: 4 ->  4   10:00:00:60:69:04:01:94   deskew 16 Master
    5 ->  5   10:00:00:60:69:04:01:94   deskew 15
    7 ->  7   10:00:00:60:69:04:01:94   deskew 17
    6 ->  6   10:00:00:60:69:04:01:94   deskew 16

 3:14 -> 14   10:00:00:60:69:04:10:83   deskew 16 Master
   15 -> 15   10:00:00:60:69:04:10:83   deskew 15
switch:admin>
```

Debugging a Trunking Failure

If a trunked ISL link fails, debugging information is available through the CLI for use in troubleshooting and error correction.

To view debugging information for a trunking ISL failure:

1. Log in to the switch as admin.
2. Enter the following command:

   `trunkdebug` *`AreaNumber1, AreaNumber2`*

`AreaNumber1`	Area number of one of the ports in the trunking group
`AreaNumber2`	Area number of another of the ports in the trunking group

   Example

   Viewing debug information for ports 3 and 5, where port 3 has not correctly configured as an E_Port:

```
switch:admin> trunkdebug 3 5
port 3 is not E port
switch:admin>
```

Frequently Asked Questions About ISL Trunking

Table 17 provides answers to some frequently asked questions regarding ISL Trunking.

Table 17: Frequently Asked Questions About ISL Trunking

Question	Answer
Does ISL Trunking replace Dense Wavelength Digital Multiplexing (DWDM)?	No, DWDM is a ring topology, and has a different function than trunking. If a DWDM ISL fails, the traffic is rerouted over alternate routes, changing the data path.
Is a Trunking master ISL the same as the Principal ISL?	No, the roles are different, although they may happen to apply to the same ISL. “Trunking master ISL” applies to the role of directing traffic over a trunking group. “Principal ISL” applies to an ISL that is used to communicate with the Principal Switch, where the Principal Switch assigns domain IDs for the fabric.
Is it possible to create a trunk between a switch and a SAN device, such as host or storage?	No; ISL Trunking is supported only for inter-switch links.
Is there a limit on the number of trunking groups on one switch?	No, the number of trunking groups that can be implemented on a switch is limited only by the number of available ports.
Are trunks automatically established when the ISL Trunking license is activated?	Yes, if eligible ISLs exist. Trunking capability is enabled by default on each port.
What happens if a slave ISL fails?	The traffic is redistributed over the remaining ISLs in the group.
What happens if a master ISL fails?	A new master ISL is designated and traffic is redistributed. If any in-flight frames are lost, there is a brief pause in the I/O.
Should port statistics be the same across all participating ISLs within a trunk?	No, although port statistics are usually fairly evenly balanced, they can vary with payload variations at the frame level.
Which Extended Fabric Modes are supported?	“L0” mode, which is the default mode. If the ports in the potential trunking group use any other modes, the trunking group does not form.
Is trunking supported for 1 Gbit/sec?	No, trunking requires 2 Gbit/sec capacity.

Zoning Procedures

10

This chapter provides information on HP zoning procedures using Fabric OS commands, and discusses the following major topics:

License Activation

Use the `licenseshow` command to verify that the *zoning* license is installed to your switch. See "Managing Licensed Features" on page 39 for more information on activating a feature using license keys.

Zoning Commands

Table 18 lists commands used to configure and manage zoning. For detailed information on these commands, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

Table 18: Zoning Commands

Command	Description
Zone Alias Commands	
`aliadd`	Add a member to an alias
`alicreate`	Create an alias
`alidelete`	Delete an alias
`aliremove`	Remove a member from an alias
`alishow`	Display an alias in the zone database
Zone Commands	
`zoneadd`	Add a member to a zone
`zonecreate`	Create a zone
`zonedelete`	Delete a zone
`zoneremove`	Remove a member from a zone
Configuration Commands	
`cfgadd`	Add a zone to a zone configuration
`cfgcreate`	Create a zone configuration
`cfgdelete`	Delete a zone configuration
`cfgremove`	Remove a zone from a zone configuration
Zoning Management Commands	
`cfgclear`	Clear all zone configurations
`cfgdisable`	Disable a zone configuration
`cfgenable`	Enable a zone configuration

Table 18: Zoning Commands (Continued)

Command	Description
`cfgsave`	Save zone configurations in flash memory
`cfgshow`	Display the zone database
`cfgtransabort`	Abort the current zoning transaction

Managing Aliases

An alias is a logical group of ports, WWNs, or AL_PAs. Specifying groups of ports or devices as an alias makes zone configuration easier, by enabling you to configure zones using an alias rather than a long string of individual members. You can specify members of an alias using the following methods:

- Switch domain and port area number pair, for example, `2, 20`. You can view the area numbers for ports using the `switchshow` command.
- WWN (device).

These procedures change the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

Creating an Alias

To create an alias, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `alicreate "`*`aliName`*`", "`*`member; member`*`"`

   `aliName` Specify a name for the alias in quotation marks. An alias name must begin with a letter and can be followed by any number of letters, digits and underscore characters. Names are case sensitive, for example `Ali_1` and `ali_1` are different aliases. Blank spaces are ignored.

member Specify a member or list of members to be added to the alias, in quotation marks, separated by semi-colons. An alias member can be specified by one or more of the following methods:

- A switch domain and port area number pair. You can view the area numbers for ports using the `switchshow` command.
- WWN

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

Example

To create an alias:

```
switch:admin> alicreate "array1", "2,32; 2,33; 2,34; 4,4"
switch:admin> alicreate "array2", "21:00:00:20:37:0c:66:23; 4,3"
switch:admin> alicreate "loop1", "0x02; 0xEF; 5,4"
switch:admin> cfgsave
```

Adding a Member to an Alias

To add members to an alias, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

`aliadd "`*`aliName`*`", "`*`member`*`; `*`member`*`"`

aliName Specify a name for the alias in quotation marks. This alias must already exist in the zone database. Names are case sensitive, for example `Ali_1` and `ali_1` are different aliases.

member Specify a member or list of members to be added to the alias, in quotation marks, separated by semi-colons. An alias member can be specified by one or more of the following methods:

- A switch domain and port area number pair. You can view the area numbers for ports using the `switchshow` command.
- WWN.

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

Example

To add members to an alias:

```
switch:admin> aliadd "array1", "1,2"
switch:admin> aliadd "array2", "21:00:00:20:37:0c:72:51"
switch:admin> aliadd "loop1", "0x02; 0xEF"
switch:admin> cfgsave
```

Removing a Member from an Alias

To remove a member from an alias, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `aliremove "`*`aliName`*`", "`*`member; member`*`"`

aliName	Specify a name for the alias in quotation marks. This alias must already exist in the zone database. Names are case sensitive, for example `Ali_1` and `ali_1` are different aliases.
member	Specify a member or list of members to be removed from the alias, in quotation marks, separated by semi-colons. An alias member can be specified by one or more of the following methods: • A switch domain and port area number pair. You can view the area numbers for ports using the `switchshow` command. • WWN.

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

Example

To remove members from an alias:

```
switch:admin> aliremove "array1", "1,2"
switch:admin> aliremove "array2", "21:00:00:20:37:0c:72:51"
switch:admin> aliremove "loop1", "0x02; 0xEF"
switch:admin> cfgsave
```

Deleting an Alias

To delete an alias, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `alidelete "aliName"`

aliName	Specify a name for the alias in quotation marks. This alias must already exist in the zone database. Names are case sensitive, for example `Ali_1` and `ali_1` are different aliases.

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

Example

To delete an alias:

```
switch:admin> alidelete "array1"
switch:admin> cfgsave
```

Viewing Aliases in the Zone Database

To view aliases, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `alishow "pattern", mode`

pattern — A character string used to match alias names. This operand must be enclosed in quotation marks. Patterns may contain:

- Question mark (?) that matches any single character.
- Asterisk (*) that matches any string of characters.
- Ranges that match any character within the range. Ranges must be enclosed in brackets, for example, [0-9] or [a-f].

mode — Specify `0` to display the contents of the transaction buffer (the contents of the current transaction), or specify `1` to display the contents of the non-volatile memory. The default value is `0`.

If no parameters are specified, the entire zone database (both the defined and effective configuration) is displayed.

Example

Show all zone aliases beginning with `arr`:

```
switch:admin> alishow "arr*"
alias: array1  21:00:00:20:37:0c:76:8c
alias: array2  21:00:00:20:37:0c:66:23
```

Managing Zones

A zone is a region within the fabric, where switches and devices can communicate. A device can communicate only with other devices connected to the fabric within its specified zone.

You can specify members of a zone using the following methods:

- Alias names.
- Switch domain and port area number pair, for example, `2, 20`. You can view the area numbers for ports using the `switchshow` command.
- WWN (device).

These procedures change the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

Creating a Zone

To create a zone, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `zonecreate "`*`zoneName`*`", "`*`member; member`*`"`

zoneName	Specify a name for the zone in quotation marks. A zone name must begin with a letter and can be followed by any number of letters, digits and underscore characters. Names are case sensitive, for example `Zone_1` and `zone_1` are different zones. Blank spaces are ignored.

member Specify a member or list of members to be added to the zone, in quotation marks, separated by semi-colons. An zone member can be specified by one or more of the following methods:

- A switch domain and port area number pair. View the area numbers for ports using the `switchshow` command.
- WWN

Example

```
switch:admin> zonecreate "greenzone", "2,32; 2,33; 2,34; 4,4"
switch:admin> zonecreate "redzone", "21:00:00:20:37:0c:66:23; 4,3"
switch:admin> cfgsave
```

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

Adding a Member to a Zone

To add a member to a zone, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `zoneadd "zoneName", "member; member"`

   zoneName Specify a name for the zone in quotation marks. This zone must already exist in the zone database. Names are case sensitive, for example `Zone_1` and `zone_1` are different zones.

   member Specify a member or list of members to be added to the zone, in quotation marks, separated by semi-colons. A zone member can be specified by one or more of the following methods:

   - A switch domain and port area number pair. You can view the area numbers for ports using the `switchshow` command.
   - WWN.

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

Example

To add members to a zone:

```
switch:admin> zoneadd "greenzone", "1,2"
switch:admin> zoneadd "redzone", "21:00:00:20:37:0c:72:51"
switch:admin> zoneadd "bluezone", "0x02; 0xEF"
switch:admin> cfgsave
```

Removing Members from a Zone

To remove members from a zone, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `zoneremove "`*`zoneName`*`", "`*`member`*`; `*`member`*`"`

zoneName	Specify a name for the zone in quotation marks. This zone must already exist in the zone database. Names are case sensitive, for example `Zone_1` and `zone_1` are different zones.
member	Specify a member or list of members to be removed from the zone, in quotation marks, separated by semi-colons. A zone member can be specified by one or more of the following methods: • A switch domain and port area number pair. You can view the area numbers for ports using the `switchshow` command. • WWN.

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

   Example

   To remove members from a zone:

```
switch:admin> zoneremove "greenzone", "1,2"
switch:admin> zoneremove "redzone", "21:00:00:20:37:0c:72:51"
switch:admin> zoneremove "bluezone", "0x02; 0xEF"
switch:admin> cfgsave
```

Deleting a Zone

To delete a zone, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `zonedelete "zoneName"`

zoneName	Specify a name for the zone in quotation marks. This zone must already exist in the zone database. Names are case sensitive, for example `Zone_1` and `zone_1` are different zones.

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

   Example

   To delete a zone:

```
switch:admin> zonedelete "bluezone"
switch:admin> cfgsave
```

Viewing Zones in the Zone Database

To view zones in the zone database, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `zoneshow "pattern", mode`

   pattern — A character string used to match zone names. This operand must be enclosed in quotation marks. Patterns may contain:

   - Question mark (?) that matches any single character.
   - Asterisk (*) that matches any string of characters.
   - Ranges that match any character within the range. Ranges must be enclosed in brackets, for example, [0-9] or [a-f].

   mode — Specify `0` to display the contents of the transaction buffer (the contents of the current transaction), or specify `1` to display the contents of the non-volatile memory. The default value is `0`.

   If no parameters are specified, the entire zone database (both the defined and effective configuration) is displayed.

Example

Show all zones beginning with A, B, or C:

```
switch:admin> zoneshow "[A-C]*"
zone: Blue_zone 1,1; array1; 1,2; array2
zone: Bobs_zone 4,5; 4,6; 4,7; 4,8; 4,9
```

Managing Configurations

The maximum number of items that can be stored in the zoning configuration database depends on the switches in the fabric, whether or not interop mode is enabled, and the number of bytes required for each item. The number of bytes required for an item depends on the specifics of the fabric, but cannot exceed 64 bytes per item.

At 64 bytes per item you can have the following:

- 767 entries for a fabric with at least one v2.x or v3.x switch and interop mode disabled
- 383 entries for a fabric with at least one v2.x or v3.x switch and interop mode enabled
- 997 entries for a fabric consisting solely of v4.x switches and interop mode disabled
- 498 entries for a fabric consisting solely of v4.x switches and interop mode enabled

You can use the `cfgSize` command to check both the maximum available size and the currently saved size. If you believe you are approaching the maximum, you can save a partially completed zoning configuration and use the `cfgSize` command to determine the remaining space

Creating a Configuration

To create a configuration, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `cfgcreate "cfgName", "member; member"`

   cfgName — Specify a name for the configuration in quotation marks. A configuration name must begin with a letter and can be followed by any number of letters, digits and underscore characters. Names are case sensitive, for example `Cfg_1` and `cfg_1` are different configurations. Blank spaces are ignored.

   member — Specify a member or list of members to be added to the configuration, in quotation marks, separated by semi-colons. A configuration member can be specified by one or more of the following methods:

   - Zone names
   - FA (Fabric Assist) zone names

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command

   Example

   To create a configuration:

```
switch:admin> cfgcreate "NEW_cfg", "redzone; bluezone; greenzone"
switch:admin> cfgsave
```

Adding Members to a Configuration

To add members to a configuration, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `cfgadd "cfgName", "member; member"`

   cfgName — Specify a name for the configuration in quotation marks. This configuration must already exist in the zone database. Names are case sensitive, for example `Cfg_1` and `cfg_1` are different configurations.

member — Specify a member or list of members to be added to the configuration, in quotation marks, separated by semi-colons. A configuration member can be specified by one or more of the following methods:

- Zone name
- FA (Fabric Assist) zone name

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

Example

To add a member to a configuration:

```
switch:admin> cfgadd "newcfg", "bluezone"
switch:admin> cfgsave
```

Removing a Member from a Configuration

To modify the members of a configuration, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

`cfgremove "`*`cfgName`*`", "`*`member`*`; `*`member`*`"`

cfgName — Specify a name for the configuration in quotation marks. This configuration must already exist in the zone database. Names are case sensitive, for example `Cfg_1` and `cfg_1` are different configurations.

member — Specify a member or list of members to be removed from the cfg, in quotation marks, separated by semi-colons. A configuration member can be specified by one or more of the following methods:

- Zone names
- FA (Fabric Assist) zone names

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

Example

To remove `redzone` from a configuration:

```
switch:admin> cfgremove "newcfg", "redzone"
```

Deleting a Configuration

To delete a configuration, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `cfgdelete "cfgName"`

cfgName	Specify a name for the configuration in quotation marks. This configuration must already exist in the zone database. Names are case sensitive, for example `Cfg_1` and `cfg_1` are different configurations.

3. Save the change to the Defined Zone Database by issuing the `cfgsave` command.

   Example

   To delete a configuration:

```
switch:admin> cfgdelete "testcfg"
switch:admin> cfgsave
```

Viewing Configurations in the Zone Database

To view a configuration in the zone database, perform the following steps:

1. Log in to the switch as admin.
2. Enter the following command:

   `cfgshow "pattern", mode`

   pattern — A character string used to match configuration names. This operand must be enclosed in quotation marks. Patterns may contain:

   - Question mark (?) that matches any single character.
   - Asterisk (*) that matches any string of characters.
   - Ranges that match any character within the range. Ranges must be enclosed in brackets, for example, [0-9] or [a-f].

   mode — Specify `0` to display the contents of the transaction buffer (the contents of the current transaction), or specify `1` to display the contents of the non-volatile memory. The default value is `0`.

   If no parameters are specified, the entire zone database (both the defined and effective configuration) is displayed.

Example

To show all zone configuration information:

```
switch:admin> cfgshow
Defined configuration:
  cfg:   new1    Blue_zone
  cfg:   NEW_cfg Red_zone; Blue_zone
  zone:  Blue_zone
     1,1; array1; 1,2; array2
  zone:  Red_zone
     1,0; loop1
  alias: array1  21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
  alias: array2  21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
  alias: loop1   21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
  cfg:   NEW_cfg
  zone:  Blue_zone
      1,1
      21:00:00:20:37:0c:76:8c
      21:00:00:20:37:0c:71:02
      1,2
      21:00:00:20:37:0c:76:22
      21:00:00:20:37:0c:76:28
   zone:  Red_zone
      1,0
      21:00:00:20:37:0c:76:85
      21:00:00:20:37:0c:71:df
```

To show only configuration names:

```
switch:admin> cfgshow *
 cfg:   a_cfg1 zone1; zone2
 cfg:   b_cfg2 zone1; zone2; zone3

switch:admin>
```

Using Interoperability Mode

11

This chapter provides information on setting up a heterogeneous fabric; that is, a fabric that includes both HP switches and other manufacturers' switches by discussing the following major topics:

About Interoperability Mode

The Interoperability mode enables HP switches and other manufacturers' switch fabrics to exchange interoperability parameters in such a way that both fabrics merge and form one single fabric with one principal switch and all unique domain IDs.

In a heterogeneous fabric, some features are not available in order to provide maximum compatibility between switches.

Use the `interopmode` command to enable or disable interoperability mode for individual HP switches. This feature enables other manufacturers' switches to be used in an HP fabric.

This command must be executed on all HP switches in the fabric. The switch must be rebooted after changing interoperability mode. Other manufacturers' switches may require the execution of one or more commands that select interoperability mode for their switches.

Note: Interoperability has been tested only on McData switches.

HP Switch Requirements

The following are HP switch requirements:

- Interoperability Mode cannot be guaranteed for firmware earlier than v4.x (for SAN Switches 2/32, 2/8V, 2/16V, Core Switches 2/64 and 2/128), v3.1x (for 2 GB series switches), and v2.6.2x (for 1 GB series switches).
- A Zoning license and a Fabric license must be installed on each HP switch.

Note: Interoperability mode does not support Enhanced Edge PID mode.

Supported HP Features

The following features are supported in a heterogeneous on HP switches only:

- HP Fabric Watch
- HP Fabric Access API functions can be accessed from HP switches only, but other manufacturers' switch information is reported. The object information and zoning actions are configurable from the API.
- HP translative mode, which registers private storage target devices into the fabric, can be used in a heterogeneous fabric as long as the devices are directly connected to HP switches. The devices are accessible from any port on the fabric.

Unsupported HP Features

In a heterogeneous fabric, the following HP optional features are not supported and cannot be installed on any switch in the Fabric:

- Extended Edge PID format
- Secure Fabric OS
- Timer Server function
- Open E-port
- Broadcast Zoning
- Management Server Service
- Remote Switch
- Extended Fabrics
- Trunking
- Alias Server
- Platform Service
- Virtual Channels
- FC-IP

Configuration Recommendations

HP recommends the following when you configure an interoperable fabric:

- Avoid Domain ID conflicts before fabric reconfiguration. There should not be duplicate domain IDs for switches joining the fabric.
- When adding multiple switches to a fabric, wait for a fabric reconfiguration after adding each switch.
- When removing multiple switches from the fabric, wait for a fabric reconfiguration after removing each switch.

Configuration Restrictions

In interoperable fabrics, the following restrictions apply:

- There is an architecture maximum of 31 switches. However, the actual configuration tested is less.
- Domain IDs must be in the 97 to 127 value range for successful connection to McData switches. The firmware automatically assigns a valid domain ID, if necessary, when the `interopmode` command is enabled on the switch.
- The `fabricshow` command shows only the WWN and Domain ID for McData. There is nothing for IP, FC-IP or name. HP switches show all of the above.
- When in Interoperability mode, all HP switches must have at least one direct connection to another HP switch. So, for example, you cannot have an HP switch connected only to a McData switch.
- LC IBM GBICs are not supported if they are to be connected to a McData ISL.
- When an HP switch gets a new domain ID assigned through a fabric reconfiguration, it writes the new domainID to flash memory and the old domain ID value is overwritten. When a McData switch gets a new domainID assigned through a fabric reconfiguration, it keeps the original domainID in flash memory. So then, when the domainID of a McData switch and an HP switch is changed via fabric reconfiguration, on the next and subsequent fabric reconfiguration, the HP switch tries to use the new ID (from flash memory) while McData tries to use its old ID (from flash memory).

  This situation may cause a domain ID overlap to occur during multiple fabric reconfigurations. Domain ID overlap is not supported for HP / McData interoperability.
- In Interoperability mode, one HP switch or fabric can be connected to one McData switch or fabric.

- In Interoperability mode, more than one ISL can be connected between HP switches.

Zoning Restrictions

Zoning has the following restrictions in interoperable fabrics:

- Only Zoning by port WWN is allowed.That means using the device's port WWN, for example, 10:00:00:00:c9:28:c7:c6.
- Zone members specified by node WWN are ignored.
- Zone configurations that use either physical port numbers or port IDs are not supported in interopmode. Zoning using port number uses the actual physical port numbers on the switch, for example slot 1, port 5. Zoning using port ID uses the device ID, for example, 010100.
- When no zoning configuration is in effect, the default effective configuration is that all ports are isolated and traffic is not permitted. This is in contrast to the HP standard behavior—when interoperability mode is off—where all data traffic is enabled.
- The SAN Switch 2/8-EL, SAN Switch 2/16, and SAN Switch 2/32 provide hardware enforcement of the port WWN zones only for devices attached to its ports. Devices attached to end-ports on other manufacturers' switches or HP StorageWorks 1 GB series switches are enforced by Name Server (soft) zoning only.
- Web Tools can be used for zone configuration as long as HP switches are directly connected to each other. If Web Tools is used to set up zoning, then Web Tools must be used as the only zone management method.
- HP switches behind a McData switch receive only the effective configuration when a zone merge occurs. This is because McData only has an effective configuration and discards the defined configuration when it sends merge information to the HP switch. However, a zone update sends both defined and effective configurations to ALL switches. All HP switches must have a direct connection to the HP fabric.
- When the HP StorageWorks Core Switch 2/64 is reconfiguring, do NOT call any zoning commands that are supposed to propagate until the fabric routes are FULLY set up. Use the `fabricshow` command to verify that all of the fabric routes are set up and all of the switch IP addresses and names are present. This does not apply to McData because it shows only the WWN and domainID.

- The maximum number of items that can be stored in the zoning configuration database depends on the switches in the fabric, whether or not interop mode is enabled, and the number of bytes required for each item. The number of bytes required for an item depends on the specifics of the fabric, but cannot exceed 64 bytes per item.

  At 64 bytes per item you can have

  — 767 entries for a fabric with at least one 2.x or 3.x switch and interop mode disabled

  — 383 entries for a fabric with at least one 2.x or 3.x switch and interop mode enabled

  — 997 entries for a fabric consisting solely of 4.x switches and interop mode disabled

  — 498 entries for a fabric consisting solely of 4.x switches and interop mode enabled

  You can use the `cfgSize` command to check both the maximum available size and the currently saved size. If you believe you are approaching the maximum, you can save a partially completed zoning configuration and use the `cfgSize` command to determine the remaining space.

Note: When interop mode is in effect, the space available for the configuration database is only half the normal size.

Zone Name Restrictions

The name field must contain the ASCII characters that actually specify the name, not including any required fill bytes. Names must adhere to the following rules:

- A name must be between 1 and 64 characters in length.
- All characters must be 7 bit ASCII characters.
- The first character of a given name must be a letter. A letter is defined as either an uppercase (A-Z) character or a lowercase (a-z) character.
- Any character other than the first character must be a lower case character (a-z), an upper case character (A-Z), a number (0-9), or one of the following symbols ($ - ^ _).

Pre-Configuration Planning

Before enabling interoperability mode, the individual fabrics should be inspected for compatibility.

- Zones should be inspected to ensure that they meet the zone criteria and restrictions. See “Zoning Restrictions” on page 225.
- Remove or disable any unsupported optional features.
- Disable the Platform Management functions using the `msplmgmtdeactivate` command.

Enabling Interoperability Mode

To enable interoperability mode:

1. Verify that you have implemented all the HP prerequisites necessary to enable interoperability mode on the fabric. See “Configuration Restrictions” on page 224 and “Pre-Configuration Planning” on page 227.
2. Log in to the switch as admin.
3. Disable the first switch, using the `switchdisable` command.
4. Issue the `interopmode 1` command to enable interoperability. This command resets a number of parameters and enables interactive mode.
5. At the `do you want to continue?` prompt, enter `yes`.
6. Reboot the switch after changing the interoperability mode.

Example

```
switch:admin> switchdisable
switch:admin> interopmode 1
The switch effective configuration will be lost when the operating mode is
changed; do you want to continue? (yes, y, no, n): [no] y done.
Interopmode is enabled

Note: It is recommended that you reboot this switch for the new change to
take effect.
switch:admin>
```

7. Repeat this procedure on all HP switches in the fabric.
8. Other manufacturers’ switches may require the execution of a similar command to enable interoperability.

9. After you have enabled interoperability mode on the HP switches and other manufacturer' switches, you can cable the other manufacturers' switches into the HP fabric, one at a time.

Disabling Interoperability Mode

To disable interoperability mode:

1. Log in to the switch as admin.
2. Issue the `switchdisable` command to disable the switch.
3. Issue the `interopmode 0` command to disable interoperability. This command resets a number of parameters and disables interactive mode.
4. At the `do you want to continue?` prompt, enter `yes`.
5. Reboot the switch after changing the interoperability mode.

Example

```
switch:admin> switchdisable
switch:admin> interopmode 0
The switch effective configuration will be lost when the operating mode is
changed; do you want to continue? (yes, y, no, n): [no] y
done.
Interopmode is disabled

Note: It is recommended that you reboot this switch for the new change to
take effect.
switch:admin>
```

6. Wait for a fabric reconfiguration after adding each switch.
7. Repeat this procedure on all HP switches in the fabric.

Selecting a Switch PID Format

12

This chapter provides information about the various switch port identifier (PID) formats used on HP StorageWorks switches, and procedures for changing the PID format, including best practices for updating an existing production SAN to a new PID format. This chapter discusses the following major topics:

Understanding Switch PID Format

A PID is a Port Identifier. PIDs are used by the routing and zoning services in Fibre Channel fabrics to identify ports in the network. They are not used to uniquely identify a device; this is done using the World Wide Name (WWN).

Some device drivers map logical disk drives to physical Fibre Channel counterparts by PID. An example in a Windows HBA driver is “Drive E: = PID 011F00”. Most drivers can either dynamically change PID mappings or use the WWN of the Fibre Channel disk for mapping, not the PID. For example, “Drive E: = WWN 10:00:00:60:69:51:0e:8b”.

The PID is a 24-bit address built from three fields: domain, area_ID, and AL_PA. Each of the domain, area_ID, and AL_PA portions of the PID require eight bits in the address space. Because of changing requirements in Fabric OS versions, different methods of specifying the area_ID were created.

There are four types of PID formats used by the existing HP StorageWorks switches:

1. VC Encoded PID Format

   In this format, out of the 8-bit Area ID, two bits are used for VC classes; the remaining bits are set to the port number. The format accommodates up to 64 ports per switch.

2. Native PID Format

   This is the format defined by the HP StorageWorks 1 GB switches, and is also the format carried forward by the HP StorageWorks 2 GB switches. This format allows the two series of products to fully interoperate. The upper four bits out of the 8-bit Area ID are set to 0001, and the remaining bits are set to the port number. The format can accommodate only up to 16 ports per switch.

3. Core Switch PID Format

   This is the format defined by the HP StorageWorks Core Switch 2/64, and is the format used by some other series products to interoperate with Core Switch 2/64. This format takes advantage of all the 8-bit address space and directly uses port number as the Area ID. It supports up to 256 ports per switch.

4. Extended Edge PID Format

   All switches in a fabric must use the same PID format. If you change the PID format of switches in an existing fabric from Native PID format to Core PID format—perhaps to add a high port-count switch—the PIDs change; you might need to reboot your servers for them to reflect the new addresses. The

Extended Edge PID format generates the same PID for a port on switches with 16 ports or less as would Native PID format, but also supports up to 128 ports per domain. This means that you can change the switches in a fabric from Native PID format to Extended Edge PID format without rebooting your hosts.

In the Extended Edge PID format, Area_ID = port-number + 0x10 and is then masked to eight bits. So the Area_ID of port 0 is 0x10; for port 111, 0x7F; for port 112, 0x00; and for port 127, 0x0F.

Extended Edge PID is supported in Fabric OS v2.6.2 and later, v3.1.2 and later, and v4.2.x and later.

Note: In addition to the four PID formats described above, Interop mode supports additional PID formats. Those formats are not discussed in this chapter.

Selecting a PID format

All switches in a fabric must use the same PID format. If you add a switch using a different PID format to a fabric, the switch segments from the fabric. The mode you select for your fabric depends on the mix of Fabric OS v2.x, v3.x and v4.x switches in the fabric, and to an extent on the specific releases of Fabric OS in use (for example, Extended Edge PID format is available only in Fabric OS v2.6.2 and later, Fabric OS v3.1.2 and later, and Fabric OS v4.2 and later).

Table 19 shows various combinations of existing fabrics, new switches added to those fabrics, and the recommended PID format for that combination. The recommendations have two main purposes: to eliminate host reboots when possible, and to minimize the need for a host reboot in the future.

Table 19: PID Format Recommendations When Adding New Switches

Existing Fabric OS Versions and PID Format	Switch to be Added	Recommendations (in order of preference)
v2.x/v3.x/v4.x; VC Encoded PID	v2.x/3.x/4.x	Use VC Encoded PID for new switch. Host reboot is not required.
v2.x/v3.x; Native PID	v2.x/v3.x	1. Use Native PID format for new switch. Host reboot is not required. 2. Convert existing fabric to Extended Edge PID format, upgrading the version of Fabric OS, if necessary. Use Extended Edge PID format for new switch. Host reboot is not required. 3. Convert existing fabric to Core PID format, upgrading the version of Fabric OS, if necessary. Set Core PID format for new switch. Host reboot *is* required.
	v4.x	1. Convert existing fabric to Extended Edge PID format, upgrading the version of Fabric OS, if necessary. Use Extended Edge PID format for new switch. Host reboot is not required. 2. Convert existing fabric to Core PID format, upgrading the version of Fabric OS, if necessary. Set Core PID format for new switch. Host reboot *is* required.
v2.x/v3.x/v4.x; Core PID	v2.x/3.x/4.x	Use Core PID for new switch. Host reboot is not required.
v2.x/v3.x/v4.x; Extended Edge PID	v2.x/3.x/4.x	Use Extended Edge PID for new switch. Host reboot is not required.

If you are building a new fabric with Fabric OS v2.x, or v3.x, or v4.x, or any combination, use Core PID format to simplify port to Area ID mapping.

PID Formats and the Host Reboot Issue

In some Fibre Channel SAN environments, storage devices and host servers are bound by their Fibre Channel addresses (called PIDs) to the host operating system. In these environments, the hosts and target HBAs in a SAN need to know the full 24-bit PIDs of the hosts and targets they are communicating with, but do not care how the PIDs are determined. But, if a storage device PID is changed, the host must reestablish a new binding, which requires the host to be rebooted. (The sections "Dynamic PID" on page 233 and "Static PID" on page 234 provide more detailed information about host PID binding.)

With the higher port counts available in the Core Switch 2/64 and SAN Director 2/128, the Native PID format used in HP StorageWorks 1 GB switches and HP StorageWorks 2 GB switches running Fabric OS 3.x needed to be replaced with a format capable of addressing higher port counts. In the Native PID format, four of the eight area bits are reserved, and the port number is used for the remaining four bits. For the Core PID format, all of the eight bits are available. The port number is used to fill all eight area bits. Because the four reserved bits in the Native PID format are always set to 1, changing from Native PID format to Core PID format changes the PID.

The Extended Edge PID format breaks the pattern that the Area_ID is derived simply from the port number. By adding 0x10 to the port number, and then wrapping the result around when the result is greater than 0x7F, the Area_ID for port numbers less than 16 is the same under both Extended Edge PID formats and Native PID formats. No host or target reboots are required to switch from Native PID format to Extended Edge PID format.

If you need to make a change to the PID format on a fabric and the change might cause the PIDs to change, follow the directions in the section "Moving to Extended Edge PID Format" on page 236 to change to Extended Edge PID format, or follow the directions in "Moving to Core PID Format" on page 248 to change to Core PID format.

Dynamic PID

WWN or dynamic PID binding is most typically used. In this case, changing the device's PID does not affect the mapping. However, before updating the PID format, it is necessary to determine whether or not any devices in the SAN bind by PID (see "Evaluating the Fabric" on page 249).

Static PID

For those few drivers that use static PID binding, when the format is changed, the mapping breaks and must be manually fixed. This can be done by rebooting the host, or using a manual update procedure on the host.

To manually correct broken mapping due to static PIDs, see the following sections for more detail:

- "Evaluating the Fabric" on page 249 discusses in more detail the process of updating to a new PID format. This starts with evaluating a production SAN to see which, if any, devices bind by PID. Then either an online or offline update procedure is chosen to perform the actual update.
- "Performing Disruptive PID Format Changes" on page 255 provides examples of step-by-step instructions for certain PID-bound devices. These procedures are applicable to any of a broad class of routine maintenance tasks; indeed, they would apply to these devices in many scenarios, with any Fibre Channel switch in any addressing mode.

As a general rule, do not use drivers that bind by PID. There are several routine maintenance procedures which might result in a device receiving a new PID. Examples include, but are not limited to:

- Changing Compatibility Mode settings
- Changing switch domain IDs
- Merging fabrics
- Relocating devices to new ports or new switches (that is, for Add, Move, Change type operations)
- Updating the core PID format
- Using hot spare switch ports to deal with failures

In every case where devices bind by PID, any such procedure becomes difficult or impossible to execute without downtime.

In some cases, device drivers let you manually specify persistent bindings by PID. In these cases, such devices must be identified and an appropriate update procedure created. If possible, the procedure should involve changing from PID binding to WWN binding.

Changes to Configuration Data

Caution: After changing the fabric PID format, if the change invalidates the configuration data (see Table 19 to determine), do not download (`configDownload`) old (pre-PID format change) configuration files to any switch on the fabric.

The PID is used to identify ports in a number of switch configuration databases (for example, the zoning configuration data uses the PID) and is used to label ports for saved data, such as performance monitor data.

Some combinations of PID format transitions invalidate configuration databases and invalidate stored data. On the switch, the databases are automatically rebuilt, but saved configuration files (files generated by the `configDownload` command, for example) now contain out of date configuration data.

Table 20 lists various combinations of before and after PID formats and indicates whether the configuration is affected.

Table 20: Combinations of Before and After PID Format and Configuration Changes

<table>
<tr><th>PID Format Before Change</th><th>PID Format After Change</th><th>Configuration Effect</th></tr>
<tr><td>Native</td><td>Extended Edge</td><td>No impact</td></tr>
<tr><td>Extended Edge</td><td>Native</td><td>No impact</td></tr>
<tr><td>Native</td><td>Core</td><td rowspan="4">You must:
Reenable zoning, if there is an active zone set.
If Destination ID (DID) binding is used, reconfigure persistent binding, and reconfigure DID list for performance monitor.</td></tr>
<tr><td>Core</td><td>Extended Edge</td></tr>
<tr><td>Core</td><td>Native</td></tr>
<tr><td>Extended Edge</td><td>Core</td></tr>
</table>

After changing the fabric PID format and verifying correct fabric operation, resave configuration data by running the `configUpload` command.

Moving to Extended Edge PID Format

This section details the steps needed to move a fabric to Extended Edge PID format, including the cases where you are moving the fabric because you are replacing an existing switch, adding a new switch, or with no switch changes.

The basic steps are:

1. Determine whether the current switch firmware versions meet the minimum supported version levels.

   Table 21 lists the minimum Fabric OS version levels supporting Extended Edge PID format. Use this table to determine if the switches in your fabric need a firmware update before changing the PID format.

Table 21: Minimum FOS Version Levels for Extended Edge PID Format

HP StorageWorks 1 GB Switches	SAN Switch 2/8-EL and SAN Switch 2/16	SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, Core Switch 2/64, SAN Director 2/128
v2.6.2	v3.1.2	v4.2.x

2. Update switch firmware as necessary.

   You can use either the command line interface or Web Tools to update the switch firmware. See the section "Updating Firmware Using the Command Line" on page 237 for directions on using the command line, or the section "Updating Firmware Using Web Tools" on page 239 for directions on using Web Tools.

3. Change the switch configuration in the fabric to Extended Edge PID format.

   You can use either the command line interface or Web Tools to change the PID format to Extended Edge, except that you cannot use Web Tools to change the PID format on the HP StorageWorks 1 GB switches: use the command line interface. See the section "Configuring Extended Edge PID Format Using the Command Line" on page 238 for directions on using the command line, or the section "Configuring Extended Edge PID Format Using Web Tools" on page 241 for directions on using Web Tools.

Updating Firmware Using the Command Line

Use this procedure to update the firmware:

1. Use the `nsallshow` command to verify the total number of devices in the fabric.
2. Download the correct firmware version to each switch as necessary.
3. Reboot all switches.
4. Verify that the switches form a single fabric and that all domain IDs remain the same.

Configuring Extended Edge PID Format Using the Command Line

Use this procedure to change the PID format and to verify fabric operations after the change:

1. Configure Extended Edge PID (Format 2) on each switch. (See Figure 7 for a sample `configure` command on an HP StorageWorks switch running Fabric OS 3.x, and see Figure 8 for a sample `configure` command on an HP StorageWorks switch running Fabric OS 4.x.)

```
Configure...

Fabric parameters (yes, y, no, n): [no] yes

    Domain: (1..239) [217]
    BB credit: (1..27) [16]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    SYNC IO mode: (0..10 [0]
    VC Encoded Address Mode: (0..1) [0]
    Switch PID Format : (0..2) [0] 2
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]

   Virtual Channel parameters (yes, y, no, n): [no] ^D
 Committing configuration...done.
 0x102fd500 (tshell): Apr 15 16:53:31
    WARNING CONFIG-PIDCHANGE_DISPLACE, 3, Switch PID format changed to
Displaced PID Format
```

Figure 7: Configure Command on HP StorageWorks Switch Running Fabric OS 3.x

```
Configure...

Fabric parameters (yes, y, no, n): [no] yes

    Domain: (1..239) [112]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    VC Encoded Address Mode: (0..1) [0]
    Switch PID Format: (1..2) [1] 2
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]
    BB credit: (1..16) [16]
```

Figure 8: Configure Command on HP StorageWorks Switch Running Fabric OS 4.x

2. Issue the `SwitchEnable` command on all switches.
3. Verify that all the switches form a fabric.
4. Use the `SwitchShow` command to verify that the interswitch links (ISLs) are correct and the device links are correct.
5. Use the `nsallshow` command to verify that the total number of devices is the same as those when starting this procedure.
6. For dual fabrics, repeat step 1 through step 5 for the other fabric.

Updating Firmware Using Web Tools

Use this procedure to update the firmware.

1. Launch Web Tools and log in as admin.
2. Click the **Firmware Upgrade** tab. Under **Function**, click the **Firmware Download** button. Download the correct firmware to each switch in the fabric.

   The appearance of screens is slightly different between switches running Fabric OS 3.x and switches running Fabric OS 4.x (see Figure 9 and Figure 10).

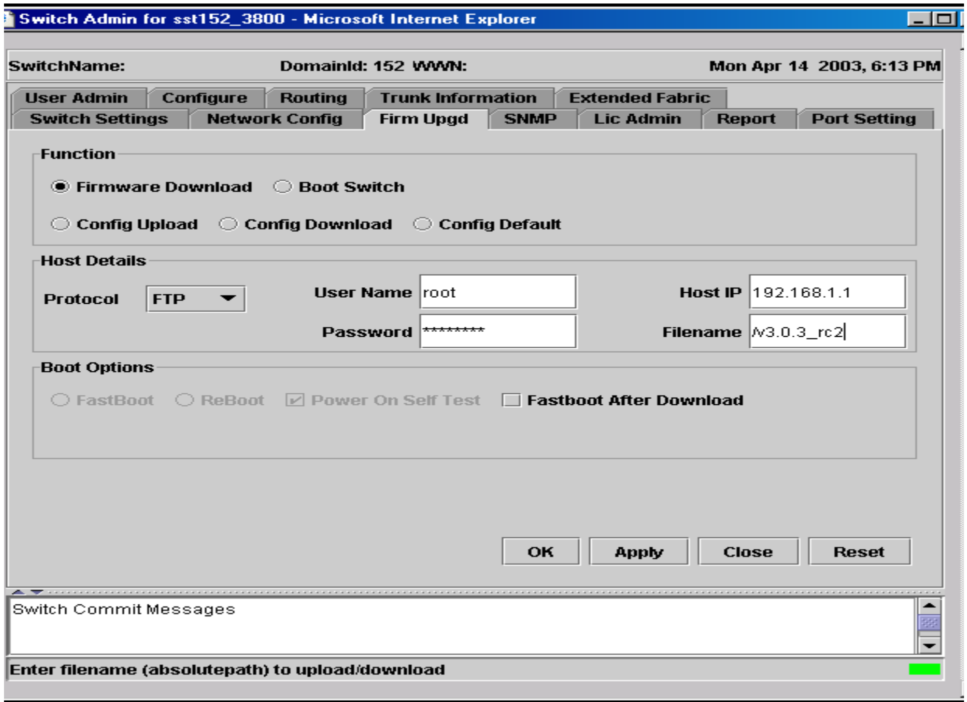

Figure 9: Firmware Download on Fabric OS v3.x

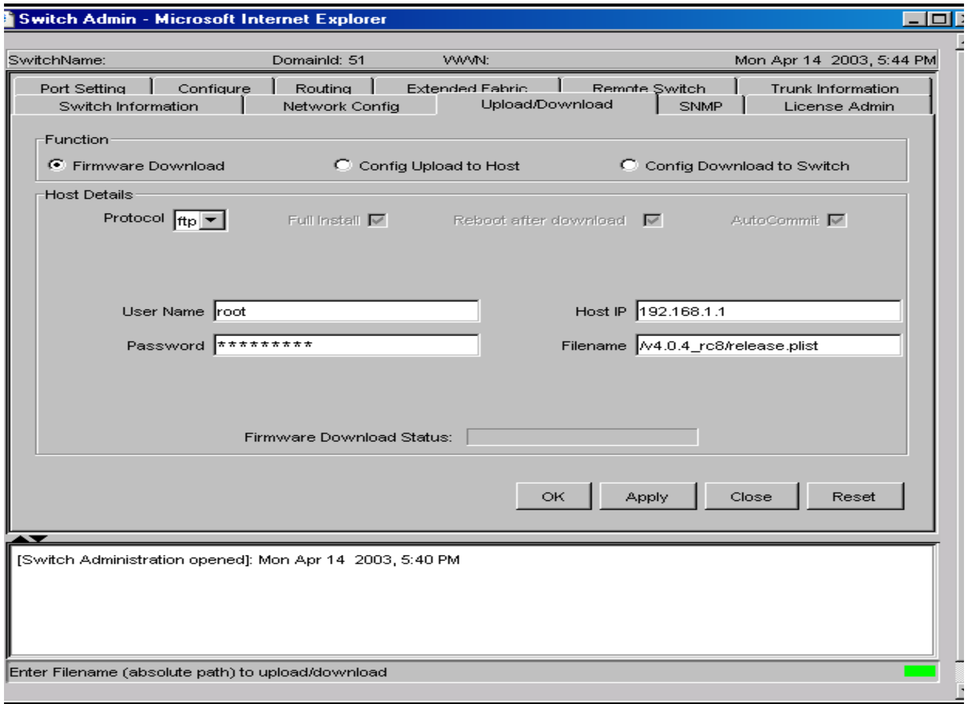

Figure 10: Firmware Download on Fabric OS v4.x

Configuring Extended Edge PID Format Using Web Tools

Note: On an HP StorageWorks 1 GB switch, you cannot use Web Tools to configure Extended Edge PID format. You must use the command line.

To configure an extended edge PID format, perform the following:

1. Click the **Configure** Tab.
2. Under **Fabric Parameters**, choose the pull-down menu and click **Format 2**.

3. Click **Apply** or **OK**. With Fabric OS 3.x, the default switch PID format is 0; with Fabric OS 4.x, the default switch PID format is 1.

   Figure 11 shows the Tab under Fabric OS 3.x; Figure 12 shows the tab under Fabric OS 4.x.

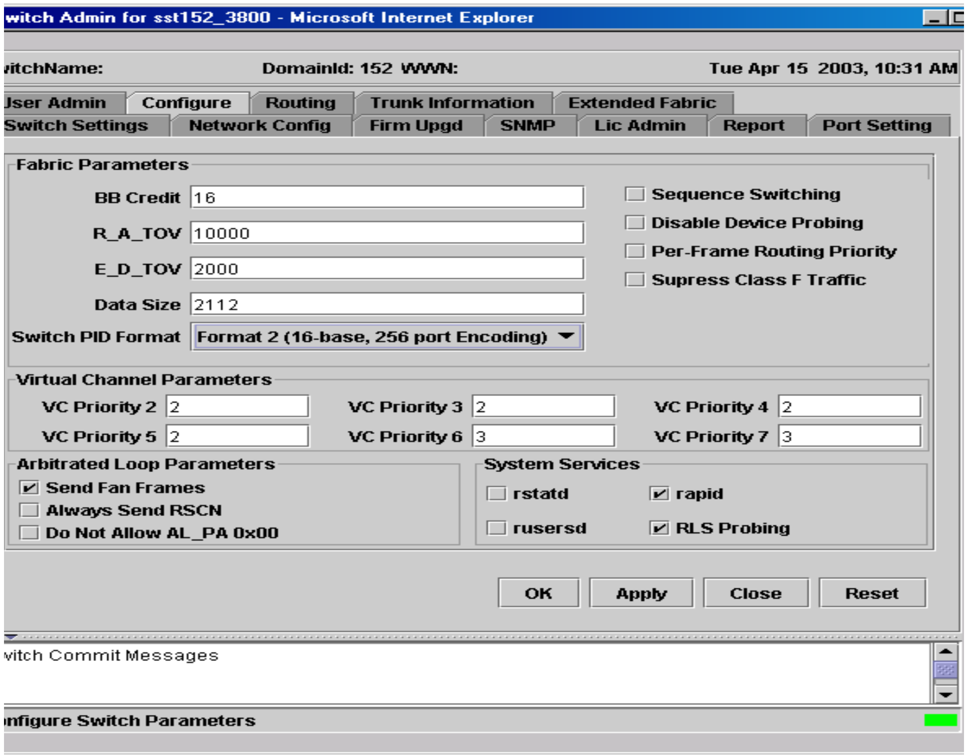

Figure 11: Select Switch PID Format 2 on Fabric OS v3.x

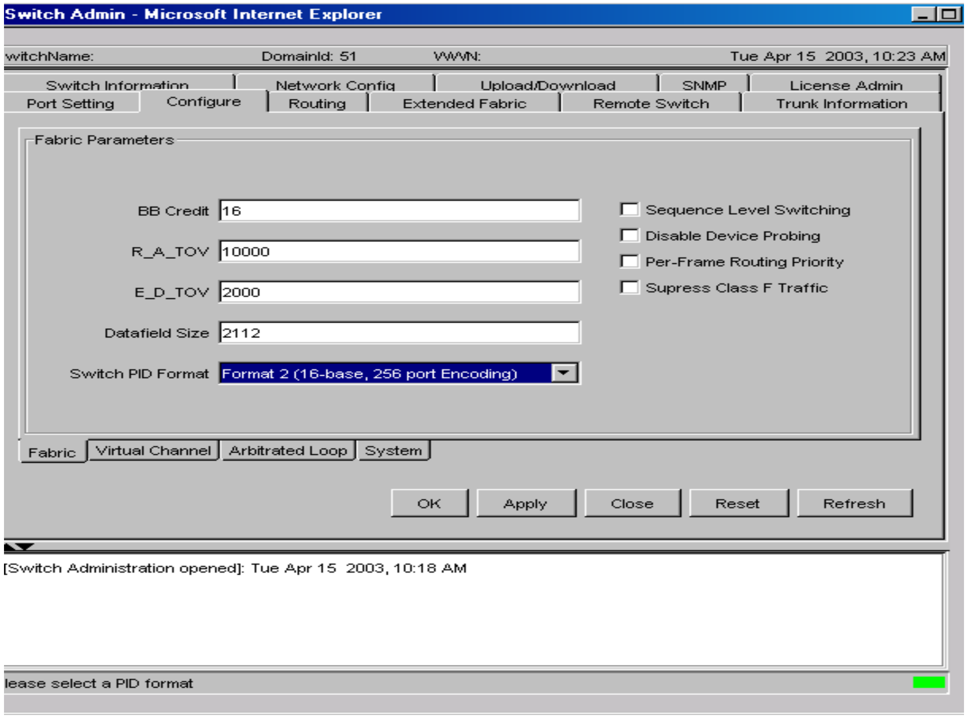

Figure 12: Select Switch PID Format 2 on Fabric OS v4.x

Migration Strategies

This section provides some recommended migration strategies for the fabric topology depicted in Figure 13, including:

- Replacing a StorageWorks SAN Switch 16 with a SAN Switch 2/32
- Inserting a SAN Switch 2/32 as an edge switch
- Inserting a SAN Switch 2/32 as a core switch

The key features of this topology are:

- A dual-fabric design, with each fabric having seven switches.
- Each host and each target has a path through fabric A and a path through fabric B.
- The hosts use static binding.

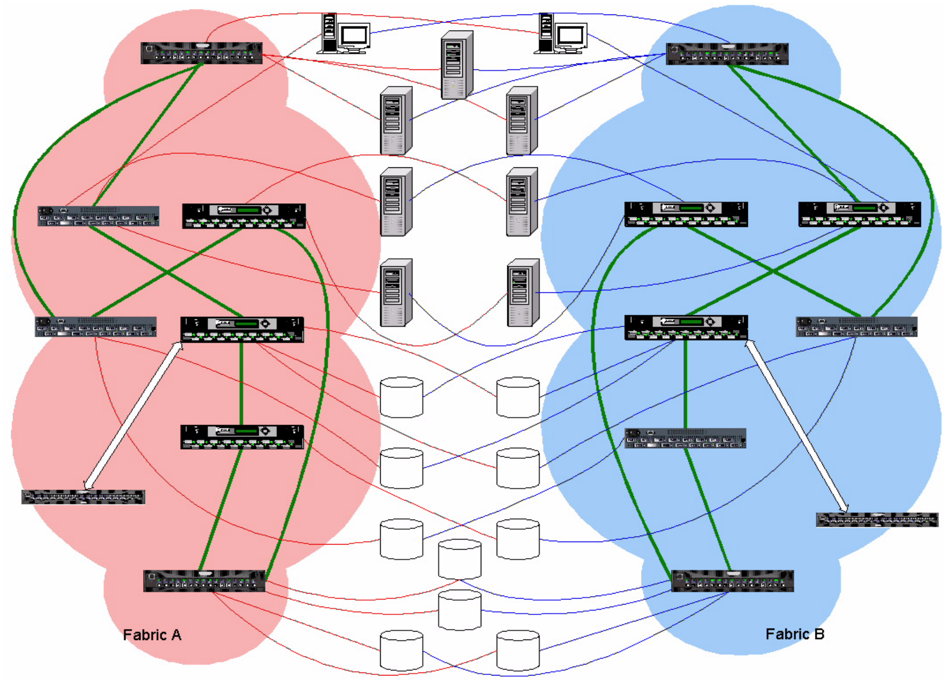

Figure 13: Sample Fabric Topology

Replacing a StorageWorks SAN Switch 16 with a SAN Switch 2/32

Use this procedure to replace a StorageWorks SAN Switch 16 with a SAN Switch 2/32 in such a way as to minimize disruption during the changeover.

1. On both fabrics, download any necessary firmware updates to each switch.
2. Set up identical zoning configurations in both fabrics. Issue the `cfgEnable` command to enable the zone set configuration.
3. Start I/O between hosts and targets.
4. Issue the `portPerfShow` command on all switches in both fabrics and verify that I/O is running between hosts and targets in the same zone.
5. Issue the `switchDisable` command on all switches in Fabric A. Verify that I/O continues on Fabric B. There should be no I/O interruption during the failover to fabric B.

6. On Fabric B: issue the `portErrShow` command to check for error frames on each switch. The fabric failover should result in minimal error frames.
7. On Fabric A:
   a. Replace the StorageWorks SAN Switch 16 with a SAN Switch 2/32 by connecting all cables to the same ports as on the replaced switch (cable from port 0 on the StorageWorks SAN Switch 16 to port 0 on the SAN Switch 2/32, and so forth).
   b. If the SAN Switch 2/32 does not already have the correct firmware version, download the correct version.
   c. Configure the same domain ID on the new SAN Switch 2/32 as was assigned to the replaced StorageWorks SAN Switch 16.
   d. Reboot all the switches.
   e. Verify that the switches form a fabric.
8. On Fabric A: configure Extended Edge PID format (Switch PID Format 2) on each switch.
9. On Fabric A: issue the `switchEnable` command on all Switches. Verify that all the switches form a fabric.
10. Issue the `switchShow` command and verify that the ISLs are correct and the device links are correct.
11. On Fabric A: issue the `nsShow` command and verify that the number of devices on the switch is identical to the corresponding switch in Fabric B.
12. On Fabric A: issue the `nsAllShow` command and verify that the total number of devices is the same as those in Fabric B.
13. Verify that I/O continues on Fabric A

Inserting a SAN Switch 2/32 as an Edge Switch

Use this procedure to add a SAN Switch 2/32 to Fabric B as an edge switch in such a way as to minimize disruption to I/O.

1. Issue the `portPerfShow` command on all switches in Fabric A.
2. Issue the `switchDisable` command on all switches in Fabric B.
3. Verify that I/O between hosts and targets in the same zone continues on Fabric A. There should be no I/O interruption due to the failover to Fabric A.
4. On Fabric A: issue the `portErrShow` command to check for error frames on each switch. The fabric failover should result in minimal error frames.

5. On Fabric B:
   a. Insert the SAN Switch 2/32 into the existing 7-switch Fabric B.
   b. As necessary, download current firmware to all switches in the fabric.
   c. Reboot all switches.
   d. Verify that the switches form a single fabric and all existing domain IDs remain the same.
6. On Fabric B: configure Extended Edge PID format (Switch PID format 2) on each switch.
7. On Fabric B: issue the `switchEnable` command on all switches.
8. Verify that all the switches form a fabric.
9. On Fabric B: issue the `switchShow` command and verify that the ISLs are correct and the device links are correct.
10. On Fabric B: issue the `nsShow` command and verify that the number of devices on each switch is identical to the corresponding switch in Fabric A.
11. On Fabric B: issue the `nsAllShow` command and verify that the total number of devices is the same as those in Fabric A.
12. Verify that I/O continues on Fabric B.
13. Issue the `portPerfShow` command on all switches in Fabric B.
14. Issue the `switchDisable` command on all switches in Fabric A.
15. Verify that I/O between hosts and targets in the same zone continues on Fabric B. There should be no I/O interruption due to the failover to Fabric B.
16. Issue the `switchEnable` command and enable all switches in Fabric A. Both fabrics are now online.
17. Issue the `nsShow` and `nsAllShow` commands and verify that the number of devices are the same in both fabrics.

Inserting a SAN Switch 2/32 as a Core Switch

Use this procedure to add a SAN Switch 2/32 to Fabric B as a core switch in such a way as to minimize disruption to I/O.

1. Issue the `portPerfShow` command on all switches in Fabric A.
2. Issue the `switchDisable` command on all the switches in Fabric B. Verify that I/O between hosts and targets in the same zone continues on Fabric A. There should be no I/O interruption due to the failover to Fabric A.

3. On Fabric A: issue the `portErrShow` command to check for error frames on each switch. The fabric failover should result in minimal error frames.
4. On the new SAN Switch 2/32:
   a. If necessary, upgrade the firmware on the SAN Switch 2/32 to the current Fabric OS v4.x.
   b. Modify the PID format from Core PID format (Format 1—the default) to Extended Edge PID format (Format 2).
   c. Disable the active zone set and clear all zone set definitions, if any.
   d. Define a unique Domain ID for the SAN Switch 2/32. (It cannot be same as any used in Fabric B.)
5. As necessary, upgrade the firmware on the switches in Fabric B.
6. Change the PID format from Native mode (Format 0) to Extended Edge mode (Format 2) on all switches in the fabric.
7. Identify each breakup point on Fabric B and disconnect all corresponding ISL links.
8. Reconnect switches with breakup points to the SAN Switch 2/32.
9. On Fabric B:
   a. Enable all edge switches.
   b. Enable the new SAN Switch 2/32.
   c. Verify that all switches form a new fabric.
10. On Fabric B: issue the `switchShow` command and verify that the ISLs and device links are correct on each switch.
11. On Fabric B: issue the `nsAllShow` command and verify that the total number of devices in the new fabric is same as before the SAN Switch 2/32 insertion.
12. On Fabric B: verify that each host can see exactly the same number of targets as Fabric A. Also, restart the I/O to any targets if they stopped due to migration.
13. Repeat this procedure on Fabric A.

Moving to Core PID Format

This section shows you how to set the PID format.

Setting the PID Format

You can set the PID format from the CLI or Web Tools. Only one format can be configured at a time. In v4.x, Native PID format is not supported. The default configuration is the Core PID format. In v2.x, Native PID format is the default configuration. In v3.x, Core PID format is the default configuration.

Note: Although the PID format is listed in the configuration file, do not change the setting directly there. Use the CLI command `configure` or Web Tools. When you use `configure` or Web Tools, switch databases that contain PID-sensitive information are automatically updated. If you change the setting in the config file and then download the edited config file, the PID format is changed, but the databases entries are not changed, and are incorrect.

When working from the CLI or Web Tools, use the following table to map the descriptive PID format names to the names used in the management interfaces:

Native PID format	Switch PID Address Mode 0
Core PID format	Switch PID Address Mode 1
Extended Edge PID format	Switch PID Address Mode 2

The VC Encode mode is either on or off. Other modes can be set only if VC Encode mode is off.

Note: Before changing the PID format, determine if host reboots are necessary. The section “Selecting a PID format” on page 231 summarizes the situations that might require a reboot. The section “PID Formats and the Host Reboot Issue” on page 233 provides more detailed information.

Example

```
switch:admin> switchdisable
switch:admin> configure
Configure...

  Fabric parameters (yes, y, no, n): [no] y

    Domain: (1..239) [1]
    BB credit: (1..27) [16]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    WAN_TOV: (1000..120000) [0]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    SYNC IO mode: (0..1) [0]
    VC Encoded Address Mode: (0..1) [0] < Must be set to 0, to use other
modes.
    Switch PID Address Mode: (0..2) [0] < Set mode number here.
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]
```

Evaluating the Fabric

If there is the possibility that your fabric has host devices with static PID bindings (See “PID Formats and the Host Reboot Issue” on page 233), you should evaluate your fabric to determine this. The fabric must be evaluated to:

- Find any devices which bind to PIDs
- Determine how each device driver responds to the PID format change
- Determine how any multi-pathing software responds to a fabric service interruption

If current details about the SAN are already available, it may be possible to skip the Data Collection step. If not, it is necessary to collect information about each device in the SAN. Any type of device may be able to bind by PID; each device should be evaluated prior to attempting an online update. This information has broad applicability, since PID-bound devices are not able to seamlessly perform in many routine maintenance or failure scenarios.

Collecting Device, Software, Hardware, and Configuration Data

The following is a non-comprehensive list of information to collect:

- HBA driver versions
- Fabric OS versions
- RAID array microcode versions
- SCSI bridge code versions
- JBOD drive firmware versions
- Multi-pathing software versions
- HBA time-out values
- Multi-pathing software time-out values
- Kernel time-out values
- Configuration of switch

Making a List of Manually Configurable PID Drivers

Some device drivers do not automatically bind by PID, but allow the operator to manually create a PID binding. For example, persistent binding of PIDs to logical drives might be done in many HBA drivers.

Make a list of all devices that are configured this way. If manual PID binding is in use, consider changing to WWN binding.

Following are some of the device types that may be manually configured to bind by PID:

- HBA drivers (persistent binding)
- RAID arrays (LUN access control)
- SCSI bridges (LUN mapping)

Analyzing Data

After you have determined the code versions of each device on the fabric, they must be evaluated to find out if any automatically bind by PID. It may be easiest to work with the support providers of these devices to get this information. If this is not possible, you may need to perform empirical testing.

Note: Binding by PID can create management difficulties in a number of scenarios. HP recommends that you not use drivers that bind by PID. If the current drivers do bind by PID, upgrade to WWN-binding drivers if possible.

The drivers shipping by default with HP/UX and AIX at the time of this writing still bind by PID, and so detailed procedures are provided for these operating systems are provided in this chapter. Similar procedures can be developed for other operating systems that run HBA drivers that bind by PID.

Note: There is no inherent PID binding problem with either AIX or HP/UX. It is the HBA drivers shipping with these operating systems that bind by PID. Both operating systems are expected to release HBA drivers that bind by WWN, and these drivers may already be available through some support channels. Work with the appropriate support provider to find out about driver availability.

It is also important to understand how multi-pathing software reacts when one of the two fabrics is taken offline. If the time-outs are set correctly, the switchover between fabrics should be transparent to the users.

Note: You should use the multipathing software to manually fail a path before starting maintenance on that fabric.

Performing Empirical Testing

Empirical testing may be required for some devices, to determine whether they bind by PID. If you are not sure about a device, work with the support provider to create a test environment.

Create as close a match as practical between the test environment and the production environment, and perform an update using the "Outline for Online Update Procedure" on page 253.

Devices that bind by PID are unable to adapt to the new format, and one of three approaches must be taken with them:

- A plan can be created for working around the device driver's limitations in such a way as to allow an online update. See the Detailed Procedures section for examples of how this could be done.
- The device can be upgraded to drivers that do not bind by PID.
- Downtime can be scheduled to reset the device during the core PID update process, which generally allows the mapping to be rebuilt.

If either of the first two options are used, the procedures should again be validated in the test environment.

Determine the behavior of multi-pathing software, including but not limited to:

- HBA time-out values
- Multi-pathing software time-out values
- Kernel time-out values

Planning the Update Procedure

Whether it is best to perform an offline or online update depends on the uptime requirements of the site.

- An offline update requires less advance planning than an online update. However, it requires that all devices attached to the fabric be offline.
- With careful planning, testing, and general due-diligence, it should be safe to update the core PID format parameter in a live, production environment. This requires dual fabrics with multi-pathing software. Avoid running backups during the update process, as tape drives tend to be very sensitive to I/O interruption.
- The online update process is intended only for use in uptime-critical dual-fabric environments, with multi-pathing software (high-uptime environments should always use a redundant fabric SAN architecture). Schedule a time for the update when the least critical traffic is running.

Note: All switches running any version of Fabric OS 4.x are shipped with the Core Switch PID Format enabled, so it is not necessary to perform the PID format change on these switches.

Migrating from manual PID binding (such as persistent binding on an HBA) to manual WWN binding and/or upgrading drivers to versions that do not bind by PID can often be done before setting the core PID format. This reduces the number of variables in the update process.

Outline for Online Update Procedure

The following steps provide SAN administrators a starting point for creating site-specific procedures.

1. Back up all data and verify backups.
2. Verify that the multi-pathing software can automatically switchover between fabrics seamlessly. If there is doubt, use the software's administrative tools to manually disassociate or mark offline all storage devices on the first fabric to be updated.
3. Verify that I/O continues over the other fabric.
4. Disable all switches in the fabric to be updated, one switch at a time, and verify that I/O continues over the other fabric after each switch disable.
5. Change the PID format on each switch in the fabric.
6. After the fabric has reconverged, issue the `cfgenable` command to update zoning.
7. Update the bindings for any devices manually bound by PID. This may involve changing them to the new PIDs, or preferably changing to WWN binding.

   For any devices automatically bound by PID, two options exist:

   - Execute a custom procedure to rebuild its device tree online. Examples are provided in the section "Performing Disruptive PID Format Changes" on page 255.
   - Reboot the device to rebuild the device tree. Some operating systems require a special command to do this, for example `boot -r` in Solaris.
8. For devices that do not bind by PID or have had their PID binding updated, mark online or reassociate the disk devices with the multi-pathing software, and resume I/O over the updated fabric.
9. Repeat this procedure with the other fabrics.

Outline for Offline Update Procedure

The following steps provide SAN administrators a starting point for creating site-specific procedures.

1. Schedule an outage for all devices attached to the fabric.
2. Back up all data and verify backups.
3. Shut down all hosts and storage devices attached to the fabric.
4. Disable all switches in the fabric.
5. Change the PID format on each switch in the fabric.
6. Reenable the switches in the updated fabric one at a time. In a core/edge network, enable the core switches first.
7. After the fabric has reconverged, issue the `cfgenable` command to update zoning (procedure provided below).
8. Bring the devices online in the order appropriate to the SAN. This usually involves starting up the storage arrays first, and the hosts last.
9. For any devices manually bound by PID, bring the device back online, but do not start applications. Update their bindings and reboot again if necessary. This may involve changing them to the new PIDs, or may (preferably) involve changing to WWN binding.
10. For any devices automatically bound by PID, reboot the device to rebuild the device tree (some operating systems require a special command to do this, such as `boot -r` in Solaris).
11. For devices that do not bind by PID or have had their PID binding updated, bring them back up and resume I/O.
12. Verify that all I/O has resumed correctly.

Hybrid Update

It is possible to combine the online and offline methods for fabrics where only a few devices bind by PID. Since any hybrid procedure is extremely customized, it is necessary to work closely with the SAN service provider in these cases.

Performing Disruptive PID Format Changes

This section includes a basic procedure that summarizes the steps necessary, but various hosts require different detailed procedures. This section includes the following topics:

- "Basic Update Procedures" on page 255
- "HP-UX" on page 257
- "AIX Procedure" on page 259

Basic Update Procedures

This process should be executed as part of the overall online or offline update process. However, it may be implemented in a stand-alone manner on a non-production fabric, or on a switch that has not yet joined a fabric.

1. Ensure that all switches in the fabric are running Fabric OS versions that support the addressing mode. HP recommends that you use v2.6.0c or later for HP StorageWorks 1 GB switches, v3.0.2c or later for HP StorageWorks SAN Switch 2/8-EL and HP StorageWorks SAN Switch 2/16 switches, and v4.0.2x or later for Core Switch 2/64.

Note: All switches running any version of Fabric OS 4.x are shipped with the Core Switch PID Format enabled, so it is not necessary to perform the PID format change on these switches.

---

2. Telnet in to one of the switches in the fabric.
3. Disable the switch by issuing the `switchdisable` command.
4. Issue the `configure` command (`configure` prompts display sequentially).
5. Enter `y` after the `Fabric parameters` prompt.
6. Enter `1` at the `Core Switch PID Format` prompt.
7. Complete the remaining prompts or press **CTRL+D** to accept the remaining settings without completing all the prompts.
8. Repeat step 2 through step 7 for the remaining switches in the fabric.
9. Reenable the switch by issuing the `switchenable` command.

Example

```
switch:admin> switchdisable
switch:admin> configure
Configure...

  Fabric parameters (yes, y, no, n): [no] yes

    Domain: (1..239) [1]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    SYNC IO mode: (0..1) [0]
    VC Encoded Address Mode: (0..1) [0] 0
    Core Switch PID Format: (0..2) [0] 1
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]
    BB credit: (1..27) [16]
```

10. After all switches are updated to use the new PID format and are reenabled, verify that the fabric has fully reconverged (each switch "sees" the other switches).
11. Issue the `cfgenable [active_zoning_config]` command on one of the switches in the fabric to update zoning to use the new PID form. This does not change the definition of zones in the fabric, but merely causes the lowest level tables in the zoning database to be updated with the new PID format setting. It is necessary to do this only once per fabric; the zoning update automatically propagates to all switches.

    At this point, all switches in the fabric are operating in the new addressing mode.

HP-UX

This procedure is not intended to be comprehensive. It provides a starting point from which you can develop a site-specific procedure for a device that binds automatically by PID, and cannot be rebooted due to uptime requirements.

1. Back up all data. Verify backups.
2. If you are not using multi-pathing software, stop all I/O going to all volumes connected through the switch/fabric to be updated.
3. If you are not using multi-pathing software, unmount the volumes from their mount points using `umount`. The proper format is `umount <mount_point>`. For example:

   ```
   umount /mnt/jbod
   ```
4. If you are using multi-pathing software, use that software to remove one fabric's devices from its configuration.
5. Deactivate the appropriate volume groups using `vgchange`. The proper format is `vgchange -a n <path_to_volume_group>`. For example:

   ```
   vgchange -a n /dev/jbod
   ```
6. Make a backup copy of the volume group directory using `tar` from within `/dev`. For example:

   ```
   tar -cf /tmp/jbod.tar jbod
   ```
7. Export the volume group using vgexport. The proper format is `vgexport -m <mapfile> <path_to_volume_group>`. For example:

   ```
   vgexport -m /tmp/jbod_map /dev/jbod
   ```
8. Log in to each switch in the fabric.
9. Issue the command `switchDisable.`
10. Issue the command `configure` and change the Core Switch PID Format to 1.
11. Issue the `cfgEnable [effective_zone_configuration]` command. For example:

    ```
    cfgEnable my_zones
    ```
12. Clean the `lvmtab` file by issuing the command `vgscan`.
13. Change to `/dev` and untar the file that was `tar`ed in step 4. For example:

    ```
    tar -xf /tmp/jbod.tar
    ```

14. Import the volume groups using `vgimport`. The proper format is `vgimport -m` *<mapfile>* *<path_to_volume_group>* *<physical_volume_path>*. For example:

    ```
    vgimport -m /tmp/jbod_map /dev/jbod /dev/dsk/c64t8d0
    /dev/dsk/c64t9d0
    ```

15. Activate the volume groups using `vgchange`. The proper format is `vgchange -a y <path_to_volume_group>`. For example:

    ```
    vgexport -a y /dev/jbod
    ```

16. If you are not using multi-pathing software, mount all devices again and restart I/O. For example:

    ```
    mount /mnt/jbod
    ```

17. If you are using multi-pathing software, reenable the affected path. The preceding steps do not clean up the results from `ioscan`. When viewing the output of `ioscan`, notice the that the original entry is still there, but now has a status of NO_HW.

```
# ioscan -funC disk
Class       I   H/W Path                       Driver S/W State   H/W Type       Description
-------------------------------------------------------------------------------------
disk        0   0/0/1/1.2.0                    adisk CLAIMED      DEVICE         SEAGATE
ST39204LC
                                               /dev/dsk/clt2d0 /dev/rdsk/c1t2d0
disk        1   0/0/2/1.2.0                    adisk CLAIMED      DEVICE         HP
DVD-ROM 304
                                               /dev/dsk/c3t2d0 /dev/rdsk/c3t2d0
disk        319 0/4/0/0.1.2.255.14.8.0         adisk CLAIMED      DEVICE         SEAGATE
ST336605FC
                                               /dev/dsk/c64t8d0 /dev/rdsk/c64t8d0
disk        320 0/4/0/0.1.18.255.14.8.0        adisk NO_HW        DEVICE         SEAGATE
ST336605FC
                                               /dev/dsk/c65t8d0 /dev/rdsk/c65t8d0
```

18. To remove the original (outdated) entry, issue the command `rmsf` (remove special file). The proper format for this command is `rmsf -a -v <path_to_device>`. For example:

    ```
    rmsf -a -v /dev/dsk/c65t8d0
    ```

19. Validate that the entry has been removed by issuing the command `ioscan -funC disk`. Notice in the example below that the NO_HW entry is no longer listed.

```
het46 (HP-50001)> ioscan -funC disk
Class      I   H/W Path                    Driver S/W State   H/W Type       Description
------------------------------------------------------------------------------------
disk       0   0/0/1/1.2.0                 adisk CLAIMED      DEVICE         SEAGATE
ST39204LC
                                           /dev/dsk/c1t2d0 /dev/rdsk/c1t2d0
disk       1   0/0/2/1.2.0                 adisk CLAIMED      DEVICE         HP
DVD-ROM 304
                                           /dev/dsk/c3t2d0 /dev/rdsk/c3t2d0
disk       319 0/4/0/0.1.2.255.14.8.0      adisk CLAIMED      DEVICE         SEAGATE
ST336605FC
                                           /dev/dsk/c64t8d0 /dev/rdsk/c64t8d0
```

20. Repeat the preceding steps for all fabrics.
21. Issue the `switchEnable` command. Enable the core switches first, then the edges.

AIX Procedure

This procedure is not intended to be comprehensive. It provides a starting point from which you can develop a site-specific procedure for a device that binds automatically by PID, and cannot be rebooted due to uptime requirements.

1. Back up all data. Verify backups.
2. If you are not using multi-pathing software, stop all I/O going to all volumes connected through the switch or fabric to be updated.
3. If you are not using multi-pathing software, vary off the volume groups. The command format is `varyoffvg` <*volume_group_name*>. For example:

   `varyoffvg datavg`

4. If you are not using multi-pathing software, unmount the volumes from their mount points using the `umount` command. The command format is `umount` <*mount_point*>. For example:

   `umount /mnt/jbod`

5. If you are using multi-pathing software, use that software to remove one fabric's devices from its configuration.

6. Remove the device entries for the fabric you are migrating. For example, if the HBA for that fabric is `fcs0`, execute the command:

   ```
   rmdev -Rdl fcs0
   ```

7. Log in to each switch in the fabric.
8. Issue the `switchdisable` command.
9. Issue the `configure` command and change the Core Switch PID Format to 1.
10. Issue the `configenable [effective_zone_configuration]` command. For example:

    ```
    configenable my_config
    ```

11. Issue the `switchenable` command. Enable the core switches first, then the edges.
12. Rebuild the device entries for the affected fabric by issuing the `cfgmgr` command. For example:

    ```
    cfgmgr -v
    ```

    This command may take several minutes to complete.

13. If you are not using multi-pathing software, vary on the disk volume groups. The proper format is `varyonvg <volume_group_name>`. For example:

    ```
    varyonvg datavg
    ```

14. If you are not using multi-pathing software, mount all devices again and restart I/O. For example:

    ```
    mount /mnt/jbod
    ```

15. If you are using multi-pathing software, reenable the affected path.
16. Repeat this procedure for all fabrics.

Frequently Asked Questions About PIDs

Q: What is a PID?

A: A PID is a Port Identifier. PIDs are used by the routing and zoning services in Fibre Channel fabrics to identify ports in the network. They are not used to uniquely identify a device; the World Wide Name (WWN) does that.

Q: What Situations Can Cause a PID to Change?

A: Many scenarios cause a device to receive a new PID. For example, unplugging the device from one port and plugging it into a different port (this might happen when cabling around a bad port, or when moving equipment around). Another example is changing the domain ID of a switch, which might be necessary when merging fabrics, or changing compatibility mode settings.

Q: Why do some devices handle a PID change well, and some poorly?

A: Some older device drivers behave as if a PID uniquely identifies a device. These device drivers should be updated if possible to use WWN binding instead. PID binding creates problems in many routine maintenance scenarios. Fortunately, very few device drivers still behave this way, and these are expected to be updated as well. Many current device drivers enable binding by PID. Select this method only if there is a compelling reason, and only after you have evaluated the impact of doing so.

Q: Must I schedule downtime for my SAN to change the PID format?

A: Only if you do not have dual fabrics or have devices that bind by PID.

Q: Must I stop all traffic on the SAN before performing the update?

A: If you are running dual fabrics with multi-pathing software, you can update one fabric at a time. Move all traffic onto one fabric in the SAN, update the other fabric, move the traffic onto the updated fabric, and update the final fabric. Without dual fabrics, stopping traffic is highly recommended. This is the case for many routine maintenance situations, so dual fabrics are always recommended for uptime-sensitive environments.

Q: How can I avoid having to change PID formats on fabrics in the future?

A: The Extended Edge PID format can be proactively set on a fabric at initial installation. The update could also be opportunistically combined with any scheduled outage. Setting the format proactively far in advance of adoption of higher port count switches is the best way to ensure administrative ease.

Diagnostics and Status

13

For detailed diagnostics information, refer to the *HP StorageWorks Diagnostics and System Error Messages 4.2.x Reference Manual*.

This chapter provides information on diagnostics and the display of switch, port, and hardware status information, and discusses the following major topics:

About Diagnostics

The purpose of the diagnostic subsystem is to evaluate the integrity of the system hardware. Diagnostics are invoked in either of two ways:

- Manually (through the Fabric OS command line)
- During the power on self test (POST)

The error messages generated during these test activities are sent to the serial console, error logs, and possibly to non-volatile storage. Each of these destinations may adjust the output format slightly to suite the purpose of the output media.

Manual Operation

During manual operation of diagnostics, the switch or blade typically needs to be in an offline state so as not to affect the fabric that the switch is placed in. There are exceptions to this policy. If a diagnostic needs the switch offline and finds that the switch is active, it does not run, and exits without harm to the fabric. Manual tests are useful in fault isolation, and in various stress test environments. There is no single test that gives a comprehensive indication of the hardware status. Tests need to be run in concert to achieve this goal.

Power on Self Test (POST)

The POST tests give a quick indication of hardware readiness when hardware is powered up. These tests do not require user input. These tests typically operate within several minutes, and support minimal validation due to the restriction on test duration. Their purpose is to give a basic health check before new hardware is allowed to join a fabric. These tests are divided into two groups: POST1 and POST2. POST1 validates the hardware interconnect of the switch/blade, and POST2 validates the ability of the switch/blade to pass data frames between the ports.

Diagnostic Command Set

The diagnostic command set can be divided into two categories:

- Control commands, which act to support or evaluate the diagnostic operations independent of performing and actual test of hardware circuitry
- Test commands, which act on hardware and report anomalies when found

There are two basic modes in which diagnostics can be manually run; they are normal interactive mode, and burn-in mode. Burn-in mode has additional control commands for its operation.

Diagnostics are also executed in the power on self test (POST) operation, but do not require user command input. They are automatically activated when Field Replaceable Units (FRUs) are brought on line.

The specific set of diagnostic and test commands run during POST depends on the switch model.

The diagnostic test commands are the following (refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more information):

- `portregtest`
- `sramretentiontest`
- `spinfab`
- `crossporttest`
- `portloopbacktest`
- `backport`
- `cmemretentiontest`
- `cmitest`
- `statstest`
- `portledtest`
- `filtertest`

The following test commands are run during POST:

- `turboramtest`
- `centralmemorytest`
- `cmitest`
- `camtest`
- `minicycle`
- `txdpath`
- `spinsilk`
- `backplanetest`

The diagnostic control commands are:

- `diagenablepost`
- `diagdisablepost`
- `diagmodeshow`
- `statsclear`
- `diagshow`
- `diagstatus`
- `diagcommandshow`
- `diaghelp`

Interactive Diagnostic Commands

When diagnostics are executed manually (from the Fabric OS command line), many commands require the switch/blade to be in an offline state. This ensures that the activity of the diagnostic does not interfere with or disturb normal fabric traffic. If the switch/blade is not in an offline state (`switchdisable`, `bladedisable`), the diagnostic command does not run and displays an error message.

No one diagnostic can give a complete assessment of the viability of all the hardware. The diagnostic commands must be used together to get an overall picture of the health of the switch or blade. If an area of the hardware is suspected of having a fault, then a set of diagnostic commands can be used to isolate and validate the functionality of the hardware.

Persistent Error Log

The Persistent Error Log feature prevents messages of lesser severity from overwriting messages of greater severity. For example, Warning messages cannot overwrite Error, Critical or Panic messages.

Features of the persistent error log include:

- The error log sub-system supports persistent logging. Each switch has its own persistent log.
- (HP StorageWorks Core Switch 2/64 and SAN Director 2/128 specific) Persistent Error Logs are saved to the current active CP and are not carried over to the new active CP in the event of a failover.
- The Persistent Error Log is preserved across power cycles and system reboots.
- The Persistent Error Log has a default capacity to store 1024 error log entries.
- The Persistent Error Log can be resized at run time without having to reboot the switch or the system.
- The Persistent Error Log can be resized at run time to configure a maximum of 2048 entries. This log can be resized to any size between 1024 and 2048 entries.

  The Error Log sub-system can save a maximum of 1536 messages in RAM, that is, a total of 256 messages for each error message level (Panic, Critical, Error, Warning, Info, and Debug). In addition, important messages are stored in a separate Persistent Error Log to guarantee that they are not lost in case of power outage or system reboot.
- The Persistent Error Log is implemented as a circular buffer. When more than the maximum entries are added to the Persistent Error Log, old entries are overwritten by new entries.
- All error messages of levels Panic and Critical are automatically saved in the Persistent Error Log as they are logged. This guarantees that Critical or Panic level messages are not lost in the event of unexpected system reboot or failover.
- A command to control and filter messages to be saved in the Persistent Error Log is provided. For example, you can specify that all log messages of level Warning or higher (basically Error, Critical, Panic*)* should be saved.
- The commands `errdump` and `errshow` display a superset of the Persistent Error Log messages saved during previous system run time cycles, and the error log messages generated during the current run time cycle.

- Options are provided to the `errdump` command to display three options: all the errors (previous Persistent Error Log and the current run time log), only errors from the current run time cycle, or the errors from the Persistent Error Log.
- Options are provided to clear the Persistent Error Log. (`errclear -p`).

Note: Only the Persistent Error Log can be resized. The run time error log cannot be resized.

Displaying the Error Log Without Page Breaks

To display the switch error log all at once:

1. Log in to the switch as admin.
2. Issue the `errdump` command.

Example

```
switch:admin> errdump

Error 04
--------
0x576 (fabos): Mar 25 08:26:44 (1)
Switch: 1, Info TRACK-LOGIN, 4, Successful login

Error 03
--------
0x576 (fabos): Mar 24 16:01:44 (12)
Switch: 1, Info TRACK-CONFIG_CHANGE, 4, Config file change from task:ZNIPC

Error 02
--------
0x2f0 (fabos): Mar 24 15:07:01
Switch: 1, Warning FW-STATUS_SWITCH, 3, Switch status changed from
HEALTHY/OK to
 Marginal/Warning

Error 01
--------
0x271 (fabos): Mar 24 15:04:06
Switch: 1, Info EM-BOOT, 4, Restart reason: Failover

switch:admin>
```

Displaying the Error Log With Page Breaks

To display the error log:

1. Log in to the switch as admin.
2. Issue the `errshow` command.

Example

```
switch:admin> errshow

Error 497
--------
0x4a5 (fabos): Oct 03 04:40:14
Switch: 0, Info TRACK-LOGIN, 4, Successful login



Type <CR> to continue, Q<CR> to stop: q
```

Clearing the Switch Error Log

To clear the switch error log for a particular switch instance:

Note: On a Core Switch 2/64 this means that both virtual switches need to be separately cleared. You need to log in to each virtual switch and perform this procedure.

---

1. Log in to the switch as admin.
2. Issue the `errclear -p` command to clear only the persistent errors. The error log in RAM is not cleared.

   Or

   Issue the `errclear` command with no operands to clear the RAM memory, and to remove persistent messages from the default `errShow` display.

   If no operand is specified, this command changes the way the error log appears in subsequent sessions. By default, the `errShow` command displays both the persistent and active log sessions. However, in future sessions you would have to use the `errShow -p` command to view persistent error messages.

The following example shows how to clear the persistent error log on the active CP.

Example

```
switch:admin> errclear -p
switch:admin>
```

Setting the Error Save Level of a Switch

To control the types of messages that are saved in the Persistent Error Log:

1. Log in to the switch as admin.
2. Issue the `errsavelvlset` command.

   The following example shows how to enable saving of Warning, Error, Critical and Panic messages in the Persistent Error Log.

Example

```
switch:admin> errsavelvlset 3
switch:admin>
```

By default, all messages of type Panic and Critical are saved in the persistent log. The argument `3` to the command specifies that all messages of severity level three or more critical should be saved. The severity levels are:

- 1 for Critical
- 2 for Error
- 3 for Warning
- 4 for Infomational
- 5 for Debug

Changes to the error save level do not persist across switch reboots.

Displaying the Current Error Save Level Setting of a Switch

To find out the current value of the Persistent Error Log save level for a switch:

1. Log in to the switch as admin.
2. Issue the `errsavelvlshow` command.

The following example shows how to display current error log save level.

Example

```
switch:admin> errsavelvlshow

 Current message save level is = 3

switch:admin>
```

The following example shows how to display current error log save level on the standby CP for switch 0 of a Core Switch 2/64.The value -s is added to save the standby CP.

Example

```
switch:admin> errsavelvlshow -s 0

 Current message save level is = 3

switch:admin>
```

Resizing the Persistent Error Log

To resize the Persistent Error Log of a switch to a new size:

1. Log in to the switch as admin.
2. Issue the `errnvlogsizeset` command.

The following example shows how to resize the persistent error log to 1500 entries.

Example

```
switch:admin> errnvlogsizeset 1500

Persistent error log is resized to store 1500 entries

switch:admin>
```

Showing the Current Persistent (Non-Volatile) Error Log Configuration of a Switch

To show the current maximum size of the Persistent Error Log:

1. Log in to the switch as admin.
2. Issue the `errnvlogsizeshow` command.

The following example shows how to display Persistent Error Log configuration

Example

```
switch:admin> errnvlogsizeshow
Persistent Error Log can store 1024 entries
```

The following example shows how to display persistent error log configuration on the standby CP of a Core Switch 2/64, for switch instance 0.

Example

```
switch:admin> errnvlogsizeshow -s 0
Persistent Error     Log can store 1024 entries
```

Configuring the Syslog Daemon

The Fabric OS can be configured to use a UNIX-style `syslog` daemon (`syslogd`) process to read system events, and to forward system messages to users and/or write the events to log files on a remote UNIX host system. See "Configuring syslogd" on page 276.

syslogd Overview

Fabric OS 4.x maintains an internal log of all error messages. The internal log buffers are limited in capacity; when the internal buffers are full, new messages overwrite old messages.

Fabric OS 4.x can be configured to send error log messages to a UNIX host system that supports `syslogd`. This host system can be configured to receive error and event messages from the switch and store them in files on the computer hard drive. This enables the storage of switch error log messages on a host system and overcomes the size limitations of the internal log buffers on the switch.

The `syslogd` is a process that runs on UNIX or Linux systems that reads and logs messages to the system console, log files, or other machines and users as specified by its configuration file. Refer to the manual pages and related documentation for your UNIX host system for more information on the `syslogd` process and its capabilities.

Note that the host system can be running UNIX, Linux or any other operating system, as long as it supports standard `syslogd` functionality.

syslog Error Message Format

Below is an example of an error or event message received by the remote `syslogd` host from the Core Switch 2/64 switch.

```
Jun 4 18:53:59 sqab186 kernel: 0x299 (fabos): Switch: 0, Info
HAMKERNEL-IP_UP, 4, (session=16) Heartbeat up from standby CP
```

The first two items are the event's date and time (as known by the UNIX host machine where `syslogd` is running) and the machine name that generated the message (in this case it is the name of the Core Switch 2/64). The word *kernel* in the message is the name of the `syslogd` facility used by the switch to send error log messages to the remote host. The rest of the message is similar to the error log message output from the `errshow` command line interface on the switch.

The fields that are specific to the switch error log message are:

- ID of the task that generated the error (in the example this is `0x299`)
- Name of the task that generated the error (in the example this is `fabos`)
- Switch instance number (in the example this is `Switch 0`)
- Message severity level in word (in the example this is `Info`)
- The error message identifier consisting of the module name (in the example this is `HAMKERNEL`) and the message name (in the example this is `IP_UP`)
- Numeric value of the message severity level defined by the switch (in the the example this is `4`)
- A descriptive text string (in the example, this is `Heartbeat up from standby CP`)

Message Classification

The syslogd messages are classified according to facility and priority (severity code). This lets you take different actions depending on the error.

Fabric OS 4.x supports six message severity levels for error log messages. Table 22 provides a mapping between severity levels used by the switch and the syslogd severity levels supported by the UNIX system.

Table 22: Mapping Between Switch and Syslogd Severity Levels

Fabric OS 4.x Message severity Levels	UNIX syslogd Message Severity Levels (Numerical Value)
Panic (0)	Emergency (LOG_EMERG) (0)
Critical (1)	Alert (LOG_ALERT) (1)
Error (2)	Error (LOG_ERR) (3)
Warning (3)	Warning (LOG_WARNING) (4)
Info (4)	Info (LOG_INFO) (6)
Debug (5)	Debug (LOG_DEBUG) (7)

Syslogd CLI Commands

Table 23 lists the commands that are related to the syslogd configuration. Please refer to the help pages of these commands for more details.

Table 23: Syslogd Configuration Commands

Command	Summary
`syslogdipadd`	Add the IP address of the remote `syslogd` host to the switch.
`syslogdipremove`	Remove the IP address of the remote `syslogd` daemon from the switch.
`syslogdipshow`	Show the list of configured `syslogd` IP addresses on the switch.
`errshow`	Display messages from the error log on the switch.

Configuring syslogd

You need to both configure the remote host and enable `syslogd` on the switch.

Configuring syslogd on the Remote Host

The `syslogd` configuration on the UNIX host provides the `syslogd` daemon with instructions on how to process different messages it receives from the switch. The following are example entries in the `syslog` configuration file, `/etc/syslog.conf`, on how to store switch error log messages received from the switch. Please refer to the `syslog` related manual pages on your UNIX system for the full documentation of the `syslog` configuration file.

The following entry in `/etc/syslog.conf` causes all messages from the switch of UNIX priority warning or higher (warning, error, critical and panic messages) to be stored in the file `/var/adm/SilkWorm`.

Example

```
kern.warning /var/adm/SilkWorm
```

The following entry in `/etc/syslog.conf` causes all messages (debug, Info, warning, error, critical, and panic) from the HP StorageWorks switch to be stored in the file `/var/adm/SilkWorm`.

Example

```
kern.debug /var/adm/SilkWorm
```

The kern prefix identifies the use of the “kernel” `syslogd` facility to dispatch error log messages to the `syslogd` daemon. The placement of entries is critical to this function. See “Configuring syslogd on the Remote Host” on page 276 and “Enabling syslogd on the Switch” on page 276 for instructions.

Enabling syslogd on the Switch

This procedure explains how to configure the switch to dispatch error log messages to a remote `syslogd` host:

1. Log in to the switch as admin.
2. Issue the `syslogdipadd` command:

```
switch:admin>syslogdipadd 'IP address of the remote
syslogd host'
```

3. Verify that the IP address was entered correctly, using the `syslogdipshow` command.

The following example shows how to configure the switch to dispatch error log messages to a remote `syslogd` host whose IP address is `nnn.nnn.nnn.nnn`

Example

```
switch:admin> syslogdipadd nnn.nnn.nnn.nnn
switch:admin> syslogdipshow
syslog.IP.address.1 nnn.nnn.nnn.nnn
```

Disabling syslogd on the Switch

To disable sending of error log messages to a previously enabled remote `syslogd` host:

1. Log in to the switch as admin.
2. Issue the `syslogdipremove` command:

   ```
   switch:admin>syslogdipremove 'IP address of the remote
   syslogd host'
   ```

3. Verify that the IP address was deleted by issuing the `syslogdipshow` command

The following example shows how to disable the sending of error log messages to a previously configured remote `syslogd` host whose IP address is `nnn.nnn.nnn.nnn`.

Example

```
switch:admin> syslogdipremove nnn.nnn.nnn.nnn
```

Switch Diagnostics

The switch status can be either Healthy/OK, Marginal/Warning, or Down. The overall status of a switch is determined by the status of several individual components within the switch. For more information on how the overall switch status is determined, see the `switchstatuspolicyset` command in the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

Displaying the Switch Status

To display the overall status of a switch:

1. Log in to the switch as admin.
2. Issue the `switchstatusshow` command. The status of the switch should be Healthy/OK. If the status is Marginal/Warning or Down, the components contributing to this status are displayed.

Example

```
switch:admin> switchstatusshow
The overall switch status is Marginal/Warning
  Contributing factors:
   *  Switch Offline triggered the Marginal/Warning status

switch:admin>
```

Displaying Information About a Switch

To display switch information:

1. Log in to the switch as admin.
2. Issue the `switchshow` command. This command displays the following information for a switch:
   - Switchname, which displays the switch name
   - Switchtype, which displays the switch model and firmware version numbers
   - Switchstate, which displays the switch state: Online, Offline, Testing, or Faulty
   - Switchrole, which displays the switch role: Principal, Subordinate, or Disabled

- Switchdomain, which displays the switch Domain ID
- Switchid, which displays the embedded port D_ID of the switch
- Switchwwn, which displays the switch World Wide Name
- Switchbeacon, which displays the switch beaconing state: either ON or OFF

The `switchshow` command also displays the following information for ports on the specified switch:

- Module type: the SFP type, if a SFP is present.
- Port speed: the speed of the Port (1G, 2G, N1, N2, or AN). The speed can be fixed, negotiated, or auto negotiated.
- Port state: the port status.
- Comment, which displays information about the port. This section may be blank or may display the WWN for F_port or E_port, Trunking state, upstream or downstream status.

The following example shows the `switchshow` command output on a Core Switch 2/64.

```
switch:admin> switchshow
switchName: switch61
switchType:     10.1
switchState:    Offline
switchRole:     Disabled
switchDomain:   97 (unconfirmed)
switchId:       fffc61
switchWwn:      10:00:00:60:69:80:04:5a
switchBeacon:   OFF
blade1 Beacon:  OFF
blade3 Beacon:  OFF

Area Slot Port Gbic Speed State
=====================================
  0    1    0   id    N2   No_Light  Disabled
  1    1    1   id    N2   No_Light  Disabled
  2    1    2   --    N2   No_Module Disabled
  3    1    3   id    N2   In_Sync   Disabled
  4    1    4   id    N2   No_Light  Disabled
  5    1    5   id    N2   In_Sync   Disabled
  6    1    6   id    N2   No_Light  Disabled
  7    1    7   id    N2   No_Light  Disabled
  8    1    8   --    N2   No_Module Disabled
  9    1    9   id    N2   No_Light  Disabled
 10    1   10   id    N2   In_Sync   Disabled
 11    1   11   --    N2   No_Module Disabled
 12    1   12   id    N2   No_Light  Disabled
 13    1   13   --    N2   No_Module Disabled
 14    1   14   id    N2   No_Sync   Disabled
 15    1   15   id    N2   In_Sync   Disabled
 32    3    0   id    N2   No_Light  Disabled
 33    3    1   --    N2   No_Module Disabled
 34    3    2   id    N2   No_Light  Disabled
 35    3    3   id    N2   No_Light  Disabled
 36    3    4   id    N2   No_Light  Disabled
 37    3    5   id    N2   In_Sync   Disabled
 38    3    6   id    N2   No_Light  Disabled
 39    3    7   id    N2   No_Light  Disabled
 40    3    8   id    N2   In_Sync   Disabled
 41    3    9   id    N2   In_Sync   Disabled
 42    3   10   id    N2   In_Sync   Disabled
 43    3   11   id    N2   In_Sync   Disabled
 44    3   12   id    N2   No_Light  Disabled
 45    3   13   id    N2   No_Light  Disabled
 46    3   14   id    N2   No_Light  Disabled
 47    3   15   id    N2   No_Sync   Disabled
switch:admin>
```

The details differ for different switch models. For more information, refer to the `switchshow` command in the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

Displaying the Uptime Of the Switch

To display the uptime for a switch:

1. Log in to the switch as admin.
2. Issue the `uptime` command. This command displays the length of time the system has been in operation, the total cumulative amount of up-time since the system was first powered-on, the date and time of the last reboot, and the reason for the last reboot. The reason for the last switch reboot is also recorded in the error log.

   Example:

```
switch:admin> uptime
  4:43am  up 1 day, 12:32,  1 user,  load average: 1.29, 1.31, 1.27
switch:admin>
```

3. The last three entries show the load average over the past 1, 5, and 15 minutes.

Port Diagnostics

You can view both software and hardware statistics for a port. These topics are discussed in the following sections.

Displaying Software Statistics for a Port

Software statistics for a port include information such as port state, number of interrupts, number of link failures, number of loss of synchronization warnings, and number of loss of signal warnings.

To display the software statistics for a port:

1. Log in to the switch as admin.
2. Issue the `portshow` command:

   `portshow [`*`slotnumber`*`]/`*`portnumber`*

   where *`slotnumber`* and *`portnumber`* specify the port location you want to view. The *`slotnumber`* is not necessary for a switch without slots.

A table of software statistics for the port is displayed.

Example

```
switch:admin> portshow 3/7
portCFlags: 0x1  ENABLED
portFlags: 0x20041       PRESENT U_PORT LED
portType:  4.2.x
portState: 2    Offline
portPhys:  4    No_Light
portScn:   0
portId:    612700
portWwn:   20:27:00:60:69:80:04:5a
portWwn of device(s) connected:
        None
Distance:  normal
Speed: N2Gbps

Interrupts:        1          Link_failure: 0          Frjt:          0
Unknown:           0          Loss_of_sync: 0          Fbsy:          0
Lli:               1          Loss_of_sig:  1
Proc_rqrd:         0          Protocol_err: 0
Timed_out:         0          Invalid_word: 0
Rx_flushed:        0          Invalid_crc:  0
Tx_unavail:        0          Delim_err:    0
Free_buffer:       0          Address_err:  0
Overrun:           0          Lr_in:        0
Suspended:         0          Lr_out:       0
Parity_err:        0          Ols_in:       0
2_parity_err:      0          Ols_out:      0
CMI_bus_err:       0

switch:admin>
```

Note: For more information on the `portshow` command, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide.*

Displaying Hardware Statistics for a Port

Hardware statistics for a port include information such as number of frames received, number of frames sent, number of encoding errors received, and number of class 2 and 3 frames received.

To display the hardware statistics for a port:

1. Log in to the switch as admin.
2. Issue the `portstatsshow` command:

   `portstatsshow [`*`slotnumber`*`]/`*`portnumber`*

   where *`slotnumber`* and *`portnumber`* specify the port location you want to view. The *`slotnumber`* is unnecessary for a switch without slots.

   A table of software statistics for the port is displayed.

Example

```
switch:admin> portstatsshow 3/7
stat_wtx        0           4-byte words transmitted
stat_wrx        0           4-byte words received
stat_ftx        0           Frames transmitted
stat_frx        0           Frames received
stat_c2_frx     0           Class 2 frames received
stat_c3_frx     0           Class 3 frames received
stat_lc_rx      0           Link control frames received
stat_mc_rx      0           Multicast frames received
stat_mc_to      0           Multicast timeouts
stat_mc_tx      0           Multicast frames transmitted
tim_rdy_pri     0           Time R_RDY high priority
tim_txcrd_z     0           Time BB_credit zero
er_enc_in       0           Encoding errors inside of frames
er_crc          0           Frames with CRC errors
er_trunc        0           Frames shorter than minimum
er_toolong      0           Frames longer than maximum
er_bad_eof      0           Frames with bad end-of-frame
er_enc_out      0           Encoding error outside of frames
er_disc_c3      0           Class 3 frames discarded
open            0           loop_open
transfer        0           loop_transfer
opened          0           FL_Port opened
starve_stop     0           tenancies stopped due to starvation
fl_tenancy      0           number of times FL has the tenancy
nl_tenancy      0           number of times NL has the tenancy
switch:admin>
```

Note: For more information on the portstatsshow command, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide.*

Displaying a Summary of Port Errors

The `porterrshow` command displays a summary of port errors for all the ports in a single switch.

To display a summary of port errors for a switch:

1. Log in to the switch as admin.
2. Issue the `porterrshow` command. The display contains one output line per port.

Example

```
switch:admin> porterrshow
       frames  enc   crc  too  too  bad  enc disc link loss loss frjt fbsy
      tx    rx   in   err shrt long  eof  out   c3 fail sync sig
sig=========================================================================
 0:    22    24    0    0    0    0    0 1.5m    0    7    3    0    0    0
 1:    22    24    0    0    0    0    0 1.2m    0    7    3    0    0    0
 2:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
 3:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
 4:  149m   99m    0    0    0    0    0  448    0    7    6    0    0    0
 5:  149m   99m    0    0    0    0    0  395    0    7    6    0    0    0
 6:  147m   99m    0    0    0    0    0  706    0    7    6    0    0    0
 7:  150m   99m    0    0    0    0    0  160    0    7    5    0    0    0
 8:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
 9:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
10:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
11:     0     0    0    0    0    0    0    0    0    0    0    2    0    0
12:     0     0    0    0    0    0    0    0    0    0    0    2    0    0
13:     0     0    0    0    0    0    0    0    0    0    0    2    0    0
14:     0     0    0    0    0    0    0    0    0    0    0    2    0    0
15:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
32:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
33:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
34:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
35:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
36:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
37:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
38:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
39:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
40:   99m  146m    0    0    0    0    0  666    0    6  796    7    0    0
41:   99m  149m    0    0    0    0    0  15k    0    2  303    4    0    0
42:   99m  152m    0    0    0    0    0  665    0    2  221    5    0    0
43:   99m  147m    0    0    0    0    0  16k    0    2  144    4    0    0
44:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
45:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
46:     0     0    0    0    0    0    0    0    0    0    0    2    0    0
47:     0     0    0    0    0    0    0    0    0    0    0    0    0    0
```

Table 24 explains the types of errors counted.

Table 24: Error Summary Description

Error Type	Description
frames tx	Frames transmitted
frames rx	Frames received
enc in	Encoding errors inside frames
crc err	Frames with CRC errors
too shrt	Frames shorter than minimum
too long	Frames longer than maximum
bad eof	Frames with bad end-of-frame delimiters
enc out	Encoding error outside of frames
disc c3	Class 3 frames discarded
link fail	Link failures (LF1 or LF2 states)
loss sync	Loss of synchronization
loss sig	Loss of signal
frjt	Frames rejected with F_RJT
fbsy	Frames busied with F_BSY

Note: For more information on the `porterrshow` command, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide.*

Hardware Diagnostics

This section discusses the following topics:

- "Monitoring the Fan Status" on page 287
- "Monitoring the Power Supply Status" on page 288
- "Monitoring the Temperature Status" on page 289
- "Running Diagnostic Tests on the Switch Hardware" on page 291

Monitoring the Fan Status

To display the fan status of a switch:

1. Log in to the switch as admin.
2. Issue the `fanshow` command. The possible values for fan status are:

   `OK` – Fan is functioning correctly.

   `absent` – Fan is not present.

   `below minimum` – Fan is present but rotating too slowly or stopped.

The following example is the command output from a Core Switch 2/64.

Example

```
switch:admin> fanshow

Fan #1 is OK, speed is 2616 RPM
Fan #2 is OK, speed is 2596 RPM
Fan #3 is OK, speed is 2596 RPM
switch:admin>
```

The following example is the command output from an HP StorageWorks SAN Switch 2/32.

Example

```
switch:admin> fanshow

Fan #1 is OK, speed is 3183 RPM
Fan #2 is OK, speed is 3214 RPM
Fan #3 is OK, speed is 3214 RPM
Fan #4 is OK, speed is 3245 RPM
Fan #5 is OK, speed is 3125 RPM
Fan #6 is OK, speed is 3375 RPM
switch:admin>
```

Note: The number of fans and valid range for RPMs varies depending on the type of switch.

Monitoring the Power Supply Status

To display the power supply status of a switch:

1. Log in to the switch as admin.
2. Issue the `psshow` command. The possible values for power supply status are:

   `OK` – Power supply present and functioning correctly.

   `absent` – Power supply not present.

   `faulty` – Power supply present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).

   After the status line, a power supply identification line may be shown. If present, this line contains the manufacture date, part numbers, serial numbers, and other identification information.

The following example is the command output from a Core Switch 2/64.

Example

```
switch:admin> psshow

Power Supply #1 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0130000931
Power Supply #2 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0130000925
Power Supply #3 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0130000941
Power Supply #4 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0130000942
switch:admin>
```

The following example is the command output from a SAN Switch 2/32.

Example

```
switch:admin> psshow

Power Supply #1 is OK
0216,FF2H0000402,60-0000739-01, A,00011,SP467, F,FF2H0000402
Power Supply #2 is OK
0219,FF2Z0000258,60-0000739-01, A,,DCJ3002-01P,PP,FF2Z0000258
switch:admin>
```

Note: The number of power supply units varies depending on the type of switch.

Monitoring the Temperature Status

To display the temperature status of a switch:

1. Log in to the switch as admin.
2. Issue the `tempshow` command. This command displays current temperature readings from each of the five temperature sensors located on the main printed circuit board of the switch. The sensors are located, approximately, one in each corner, and one at the center of the PCB.

The following example is the command output from a Core Switch 2/64.

Example

```
switch:admin> tempshow

Index    Slot     State             Centigrade     Fahrenheit
==========================================================
  1        1      Ok                    44             111
  2        2      Absent
  3        3      Ok                    41             105
  4        4      Absent
  5        5      Ok                    23              73
  6        6      Ok                    24              75

switch:admin>
```

The following example is the command output from a SAN Switch 2/32.

Example

```
switch:admin> tempshow

Index    Slot     State             Centigrade     Fahrenheit
==========================================================
  1        0      Ok                    44             111
  2        0      Ok                    38             100
  3        0      Ok                    23              73
  4        0      Ok                    43             109
  5        0      Ok                    38             100

switch:admin>
```

Note: The number of temperature sensors, the location of the sensors, and the range of temperatures for safe operation varies, depending on the type of switch.

Running Diagnostic Tests on the Switch Hardware

There are several diagnostic tests you can run on a switch. For more information, refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

The following tests are generally run during the POST, each time a switch is booted up (the actual tests run depend in part on the switch model):

- camtest
- centralMemoryTest
- cmemRetentionTest
- cmiTest
- crossPortTest
- minicycle
- portLoopbackTest
- sramRetentionTest
- statsTest
- spinSilk
- turboRamTest
- txdpath

Linux Root Capabilities

You can enable Linux root capabilities for diagnostic purposes. Enabling Linux root capabilities requires the Linux Root Enabling firmware, available from the switch provider. You cannot use the Linux Root Enabling firmware to perform any other switch functions.

Have the WWN and the output of the `licenseidshow` command of your switch available when you contact your switch support provider to enable Linux capabilities for diagnostics.

Troubleshooting

14

This chapter provides information on troubleshooting and explains the most common procedures used to diagnose and repair issues.

This chapter discusses the following major topics:

The following specific scenarios are described to provide examples of troubleshooting techniques:

About Troubleshooting

Troubleshooting should begin at the center of the SAN — the fabric. Because switches are located between the hosts and storage devices, and have visibility into both sides of the storage network, starting with them can help narrow the search path. After eliminating the possibility of a fault within the fabric, see if the problem is on the storage side or the host side, and continue a more detailed diagnosis from there. Using this approach can quickly pinpoint and isolate problems.

For example, if a host cannot see a storage device, run a switch command to see if the storage device is logically connected to the switch. If not, focus first on the storage side. Use storage diagnostic tools to better understand why it is not visible to the switch. Once the storage can be seen from the switch, if the host still cannot see the storage device, then there is still a problem between the host and switch.

Port Initialization and FCP Auto Discovery Process

Figure 14 on page 296 displays the port initialization and the Fibre Channel Protocol (FCP) auto discovery process.

The steps in the port initialization process represent a protocol used to discover the type of connected device and establish the port type.

The possible port types are:

- U_PortUniversal FC port. This port type is the base Fibre Channel port type. All unidentified, or uninitiated ports are listed as U_Ports.
- FL_PortFabric Loop port. This port connects both public and private loop devices.
- G_PortGeneric port. This port acts a transition port for non-loop fabric capable devices (E_port / F_port).
- E_PortExpansion port. This port type is assigned to ISL links.
- F_PortFabric port. This port is assigned to fabric capable devices.

The HP FCP auto discovery process enables private storage devices that accept PRLI to communicate in a fabric.

If device probing is enabled, the embedded port PLOGIs and attempts a PRLI into the device to retrieve information to enter into the Name Server. This enables private devices that do not FLOGI, but do accept PRLI, to be entered in the Name

Server and receive full fabric citizenship. Private devices that accept PRLI represent a majority of storage targets. Private hosts require the QuickLoop feature, which is not available in Fabric OS v4.2.

Note: HP does not support QuickLoop at this time.

A fabric capable device implicitly registers information with Name Server during a FLOGI. These devices typically register information with the Name Server before querying for a device list. The embedded port still PLOGIs and attempts PRLI with these devices.

You can view the Name Server table in Web Tools by clicking the **Name Server** button in the Fabric toolbar. Refer to the *HP StorageWorks Advanced Web Tools 4.2.x User Guide* for more information.

Figure 14 displays the port initialization and the Fibre Channel Protocol (FCP) auto discovery process.

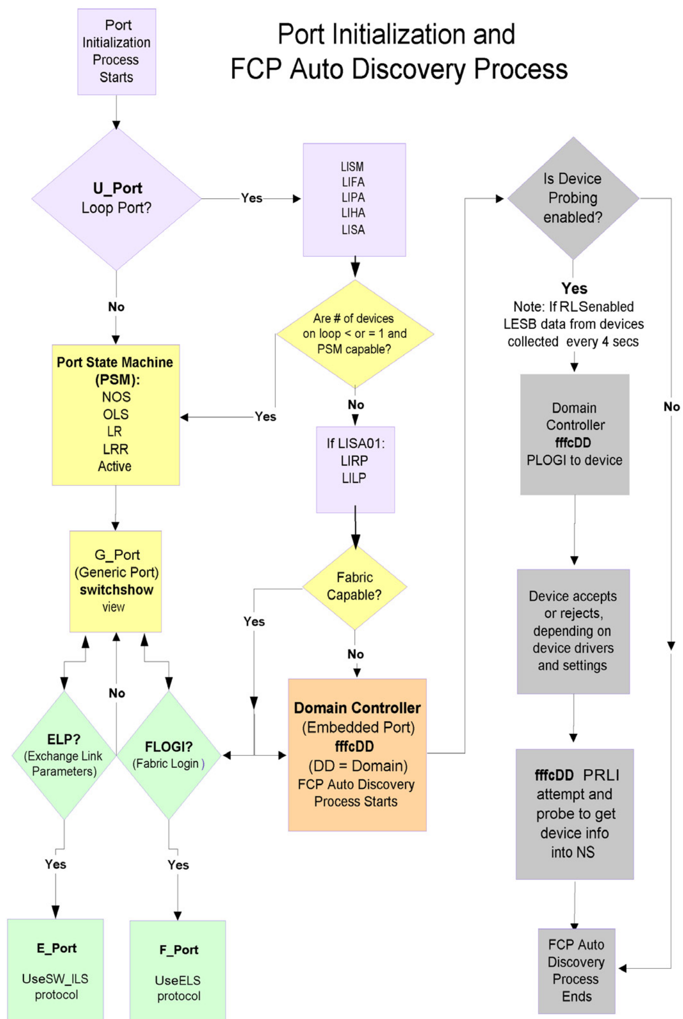

Figure 14: Port Initialization and FCP Auto Discovery Process

Most Common Problem Areas

Table 25 specifies the most common problem areas.

Table 25: Most Common Problem Areas

Area	Investigate
Fabric	Missing devices.
	Marginal links (unstable connections).
	Incorrect zoning configurations.
	Incorrect switch configurations.
Storage Devices	Physical issues between switch and devices.
	Incorrect storage software configurations.
Hosts	Incorrect Host Bus Adapter installation.
	Incorrect device driver installation.
	Incorrect device driver configuration.
Storage Management Applications	Incorrect installation and configuration of the storage devices that the software references. For example, if using a volume-management application, check for: • Incorrect volume installation • Incorrect volume configuration

There are many tools available to help troubleshoot the SAN. The following table describes tools that can be used to troubleshoot specific areas.

Table 26: Troubleshooting Tools

Problem Area	Troubleshooting Tool
Fabric	Switch LEDs
	Switch commands for diagnostics (command line)
	Web or GUI-based monitoring and management software tools
	Real-time distributed fabric operating system with advanced diagnostics
Storage Devices	Device LEDs
	Storage diagnostic tools

Table 26: Troubleshooting Tools (Continued)

Problem Area	Troubleshooting Tool
Hosts	Host adaptor LEDs
	Host operating system diagnostic tools
	Device driver diagnostic tools
Storage Management Applications	Application-specific tools and resources

Gathering Information for Technical Support

To aid in troubleshooting, gather as much of this information as possible prior to contacting the SAN technical support vendor.

1. Gather Switch Information:
   a. Serial number (located on the chassis)
   b. World Wide Name (obtain using licenseidshow or wwn commands)
   c. Fabric OS version (obtain using the `version` command)
   d. Switch Configuration settings
2. Gather Host Information:
   a. OS version and patch level
   b. HBA type
   c. HBA firmware version
   d. HBA driver version
   e. Configuration settings
3. Gather Storage Information:
   a. Disk/tape type
   b. Disk/tape firmware level
   c. Controller type
   d. Controller firmware level
   e. Configuration settings

4. Storage Software (that is, EMC Control Center, Veritas SPC, and the like)
5. SNMP management being used

Specific Scenarios

The following sections provide specific help with some of the most common SAN problems.

Host Cannot See Target (Storage or Tape Devices)

When a host cannot see its disks, the best way to troubleshoot the problem is to start in the middle half of the data path, figure out if the problem is "above" or "below" the data path, and keep dividing the suspect path in half until the problem is identified.

There are a few areas to check in the process of elimination:

- "Check the Logical Connection" on page 299
- "" on page 300
- "Check for Zoning Discrepancies" on page 302

Check the Logical Connection

1. Issue the `switchShow` command.
2. Review the output and determine if the device is logically connected to the switch:
   - A device that is logically connected to the switch is registered as an NX_Port.
   - A device that is not logically connected to the switch is registered as something other than an NX_Port.

   a. If the missing device is logically connected, move on to "" on page 300.

   b. If the missing device is not logically connected, eliminate the host and everything on that side of the data path from the suspect list.
   This includes:
      — All aspects of the host's OS
      — HBA driver settings and binaries
      — HBA Basic Input Output System (BIOS) settings

— HBA SFP
— The cable going from the switch to the host
— The SFP on the switch side of that cable
— All switch settings related to the host.

c. Go to "Link Initialization Failure (Loop)" on page 335.

Check the Simple Name Server (SNS)

1. Issue the `nsShow` command on the switch to which the device is attached and then follow the steps after the example.

Example

```
The Local Name Server has 9 entries {

 Type Pid   COS    PortName            NodeName            TTL(sec)

*N   021a00;   2,3;20:00:00:e0:69:f0:07:c6;10:00:00:e0:69:f0:07:c6; 895
    Fabric Port Name: 20:0a:00:60:69:10:8d:fd
NL   051edc;    3;21:00:00:20:37:d9:77:96;20:00:00:20:37:d9:77:96; na
    FC4s: FCP [SEAGATE ST318304FC      0005]

    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL   051ee0;    3;21:00:00:20:37:d9:73:0f;20:00:00:20:37:d9:73:0f; na
    FC4s: FCP [SEAGATE ST318304FC      0005]

    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL   051ee1;    3;21:00:00:20:37:d9:76:b3;20:00:00:20:37:d9:76:b3; na
    FC4s: FCP [SEAGATE ST318304FC      0005]

    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL   051ee2;     3;21:00:00:20:37:d9:77:5a;20:00:00:20:37:d9:77:5a; na
    FC4s: FCP [SEAGATE ST318304FC      0005]

    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL   051ee4;    3;21:00:00:20:37:d9:74:d7;20:00:00:20:37:d9:74:d7; na
    FC4s: FCP [SEAGATE ST318304FC      0005]

    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL   051ee8;    3;21:00:00:20:37:d9:6f:eb;20:00:00:20:37:d9:6f:eb; na
    FC4s: FCP [SEAGATE ST318304FC      0005]

    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL   051eef;    3;21:00:00:20:37:d9:77:45;20:00:00:20:37:d9:77:45; na
    FC4s: FCP [SEAGATE ST318304FC      0005]

    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 N    051f00;   2,3;50:06:04:82:bc:01:9a:0c;50:06:04:82:bc:01:9a:0c; na
    FC4s: FCP [EMC     SYMMETRIX       5267]

    Fabric Port Name: 20:0f:00:60:69:10:9b:5b
```

2. Look for the device in the list of the Simple Name Server. The SNS lists all of the nodes connected to that switch. This lets you determine if a particular node is accessible on the network.

- If the device is not present in the SNS, the search is narrowed to the virtual SAN cable; the problem is between the storage device and the switch. This is not a host problem, and may indicate a time-out or communication problem between the edge devices and the Name Server. Go to step 3.
- If the device is listed in the SNS, the search is narrowed; the problem is between the storage device and the host. There may be a zoning mismatch or a host/storage issue. See "Check for Zoning Discrepancies" on page 302.

3. Check the edge device documentation to determine if there is a time-out setting or parameter that may be reconfigured. If this does not solve the communication problem, contact the support organization for the product that appears to be timing out.

Check for Zoning Discrepancies

To determine if zoning might be causing a communication problem between devices:

1. Issue the `cfgShow` command to determine if zoning is enabled.

   If zoning is enabled, it is possible that the problem is being caused by a zoning conflict (that is, two devices in different zones cannot see each other).

Example

```
switch:admin> cfgshow
Defined configuration:
  cfg:   USA1    Blue_zone
  cfg:   USA_cfg Red_zone; Blue_zone
  zone:  Blue_zone
     1,1; array1; 1,2; array2
  zone:  Red_zone
     1,0; loop1
  alias: array1  21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
  alias: array2  21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
  alias: loop1   21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
  cfg:   USA_cfg
  zone:  Blue_zone
      1,1
      21:00:00:20:37:0c:76:8c
      21:00:00:20:37:0c:71:02
      1,2
      21:00:00:20:37:0c:76:22
      21:00:00:20:37:0c:76:28
   zone:  Red_zone
      1,0
      21:00:00:20:37:0c:76:85
      21:00:00:20:37:0c:71:df
```

2. Confirm that the specific edge devices that need to communicate with each other are in the same zone.
   - If they are, zoning is not causing the communication problem.
   - If they are not, and zoning is enabled, continue to step 3.
3. Resolve zoning conflicts by putting the devices into the same zoning configuration. See "Correcting Zone Merge Conflicts (Basic Procedure)" on page 308.

Fabric Segmentation

Fabric Segmentation is generally caused by one of these problems:

- Incompatible fabric parameters. See "Restoring a Segmented Fabric" on page 305.
- The Core PID not being set. The Core PID is part of fabric parameters. See Chapter 13, "Selecting a Switch PID Format" on page 255.
- Incompatible zoning configuration. See "Fabric Merge Conflicts Related to Zoning" on page 308.
- Domain ID conflict. See "Reconcile a Domain ID Conflict" on page 306.
- A switch in a secure fabric that is not running Secure Fabric OS. Refer the *HP StorageWorks Secure Fabric OS 4.2.x User Guide*.

About Fabric Parameters

There are a number of settings that control the overall behavior and operation of the fabric. Some of these values, such as the domain ID, are assigned automatically by the fabric and may differ from one switch to another in the fabric. Other parameters, such as the BB credit, can be changed for specific applications or operating environments, but must be the same among all switches to allow the formation of a fabric.

Mandatory Identical Settings

The following fabric parameters must be identical for a fabric to merge:

- R_A_TOV
- E_D_TOV
- Data Field Size
- Sequence Level Switching
- Disable Device Probing
- Suppress Class F Traffic
- VC Encoded Address Mode
- Per-frame Route Priority
- Long Distance Fabric
- BB Credit
- Core PID

Domain ID Conflicts

A domain ID conflict can occur if a switch that is in the online state is added to a fabric, and the joining switch domain ID conflicts with the domain ID of a switch in the fabric. Normally, domain IDs are automatically assigned; however, after a switch is online, the domain ID cannot change, as it would change the port addressing and potentially disrupt critical I/O.

Restoring a Segmented Fabric

The following procedure describes how to correct inconsistent fabric parameters that cause segmentation. For information on zoning configuration incompatibility, see "Fabric Merge Conflicts Related to Zoning" on page 308.

Reconcile Fabric Parameters Individually

The following procedure describes how to edit incompatible fabric parameters between fabrics by hand. To reconcile an entire configuration at once, see "Restore Fabric Parameters Through ConfigUpload" on page 306.

1. Log in to one of the segmented fabrics as admin.
2. Issue the `configshow` command.
3. Open another Telnet session and log in to the next fabric as admin.
4. Issue the `configshow` command.
5. Compare the two fabric configurations line by line and look for differences. Do this by comparing the two Telnet windows, or by printing the `configshow` output.
6. Log in to the segmented switch after the discrepancy is identified.
7. Disable the switch by issuing `switchdisable`.
8. Issue the `configure` command to edit the fabric parameters for the segmented switch.

   Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more detailed information.
9. Enable the switch by issuing the `switchenable` command.

Restore Fabric Parameters Through ConfigUpload

The following procedure describes how to restore a segmented fabric by uploading the entire correct configuration, then downloading that configuration to the segmented switch. This reconciles any discrepancy in the fabric parameters and allows the segmented switch to rejoin the main fabric. To edit and correct a configuration by hand, see "Reconcile Fabric Parameters Individually" on page 305.

1. Verify that the FTP service is running on the host workstation.
2. Log in to a switch in the known working fabric as admin.
3. Issue the `configupload` command.
4. Give the text file a relevant name and save it to a host.
5. Open a new Telnet session and log in to the segmented switch as admin.
6. Shut down the switch by issuing the `switchdisable` command.
7. Issue `configdownload`. The command becomes interactive and prompts appear for the required information.
8. Select `y` at the `Do you want to continue [y/n]` prompt. A `download complete` message displays.
9. (Optional) Use the `configure` command to preset the domain ID (as opposed to letting it be chosen at random).
10. Reboot the switch by issuing the `reboot` command.
11. Repeat this procedure on all switches that have incorrect fabric parameters.

Reconcile a Domain ID Conflict

When a domain ID conflict appears, the conflict is reported only at the point where the two fabrics are physically connected. However, there may be several conflicting domain IDs, which appear as soon as the initial conflict is resolved. Repeat the process described below until all domain ID conflicts are resolved.

1. Issue the `switchshow` command on a switch from one of the fabrics.
2. Open a separate Telnet window.
3. Issue the `switchshow` command on a switch from the second fabric.
4. Compare the `switchshow` output from the two fabrics. Note the number of domain ID conflicts; there may be several duplicate domain IDs that must be changed.

5. Chose the fabric on which to change the duplicate domain ID. Log in to the conflicting switch in that fabric.
6. Issue the `switchdisable` command.
7. Issue the `switchenable` command. This enables the joining switch to obtain a new domain ID as part of the process of coming online. The fabric principal switch allocates the next available domain ID to the new switch during this process.
8. Repeat step 5 through step 7 if additional switches have conflicting domain IDs.

Zoning Setup Issues

Refer to the *HP StorageWorks OS 4.2.x Features User Guide* for information about setting up zoning and preventing segmentation due to zoning. Table 27 and Table 28 summarize the zoning-related commands.

Table 27: Zoning Related Commands

Command	Function
`switchshow`	Displays currently enabled configuration and any E_port segmentations due to zone conflicts.
`licenseshow`	Displays current license keys and associated (licensed) products.

Table 28: Zone-Specific Commands

Command	Function
`cfgcreate`	Use to create a zone configuration.
`cfgshow`	Displays zoning configuration.
`zoneadd`	Use to add a member to an existing zone.
`zoneshow`	Displays zone information.
`zonecreate`	Use to create a zone. Before a zone becomes active, the `zonesave` and `cfgenable` commands must be used.

Table 28: Zone-Specific Commands

Command	Function
`alicreate`	Use to create a zone alias.
`alidelete`	Use to delete a zone alias.
`zonehelp`	Displays help information for zone commands.

Fabric Merge Conflicts Related to Zoning

To prevent fabric segmentation, refer to the *HP StorageWorks OS 4.2.x Features User Guide* for setup information. In addition, fabric merges can be tested prior to merging using Fabric Manager. Refer to the *HP StorageWorks Fabric Manager 4.1.1 User Guide*.

There are three types of zone configuration discrepancies that can cause segmentation, described in Table 29.

Table 29: Types of Zone Discrepancies

Conflict Cause	Description
Configuration mismatch	Occurs when zoning is enabled in both fabrics and the zone configurations that are enabled are different in each fabric.
Type mismatch	Occurs when the name of a zone object in one fabric is also used for a different type of zone object in the other fabric.
Content mismatch	Occurs when the definition of a zone object in one fabric is different from the definition of a zone object with the same name in the other fabric.

Correcting Zone Merge Conflicts (Basic Procedure)

Caution: This is a disruptive procedure. To correct a merge conflict without disrupting the fabric, see "Correcting Zone Merge Conflicts (Detailed Procedures)" on page 309, or refer to the *HP StorageWorks OS 4.2.x Features User Guide*.

To quickly correct a fabric merge problem due to incompatible zones, perform the following steps:

1. Determine which switches have the incorrect configuration. Log in to each of those switches as admin.
2. Issue the `cfgDisable` command.

Note: Be careful using the `cfgclear` command, because you can inadvertently delete the zone configuration in the fabric. Make sure you are deleting the incorrect configuration.

---

3. Issue the `cfgClear` command.
4. Issue the `switchdisable` command.
5. Issue the `switchenable` command. This automatically invokes the `cfgSave` command. The two fabrics are remerged.
6. See "Correcting Zone Merge Conflicts (Detailed Procedures)" on page 309 for more detailed troubleshooting instructions.

Correcting Zone Merge Conflicts (Detailed Procedures)

For more information regarding zoning, refer to the *HP StorageWorks OS 4.2.x Features User Guide*.

For detailed troubleshooting of zone merge issues, see the following:

- "Verify Fabric Merge Problem" on page 309
- "Edit Zone Config Members" on page 309
- "Reorder the Zone Member List" on page 310

Verify Fabric Merge Problem

1. Issue the `swithshow` command to validate that the segmentation is due to a zone issue.
2. See "Zoning Setup Issues" on page 307 to view the different types of zone discrepancies.

Edit Zone Config Members

1. Log in to one of the segmented fabrics as admin.

2. Issue the `cfgshow` command. Typing the `*` symbol after the command displays list of all config names.
3. Print the output from the `cfgShow` command.
4. Start another Telnet session and log in to the next fabric as admin.
5. Issue the `cfgShow` command.
6. Print the output from the `cfgShow` command.
7. Compare the two fabric zone configurations line by line and look for an incompatible configuration. See "Fabric Merge Conflicts Related to Zoning" on page 308 for definitions.
8. Log in to one of the Fabrics.
9. Issue zone configure editing commands to edit the fabric zone configuration for the segmented switch. Refer to the *HP StorageWorks OS 4.2.x Features User Guide* for specific commands.

Reorder the Zone Member List

If the zoneset members between two switches are not listed in the same order in both configurations, the configurations are considered a mismatch; this results in the switches being segmented in the fabric. For example:

> `[cfg1 = z1; z2]` is different from `[cfg1 = z2; z1]`, even though the members of the configuration are the same.

One simple approach to making sure that the zoneset members are in the same order is to keep the members in alphabetical order.

1. Use the output from the `cfgshow` for both switches.
2. Compare the order that the zone members are listed. Members must be listed in the same order.
3. Rearrange zone members so that the configuration for both switches is the same. Arrange zone members in alphabetical order, if possible.
4. Verify that all zone members appear to be the same, and are displayed in the same order.

MQ-WRITE Error

An MQ error is a message queue error. Identify an MQ error message by looking for the two letters M and Q in the error message.

Example

```
<switch number> Critical MQ-QREAD, 1, mqRead, queue = <?>, queue ID
= <queue ID#>, tmsg = ?>, errno = <error number>
```

MQ errors can result in devices dropping from the Simple Name Server or can prevent a switch from joining the fabric. MQ errors are rare and difficult to troubleshoot. HP recommends that you resolve them by working with the switch supplier. When MQ errors are encountered, execute the `supportShow` command to capture debug information about the switch. Then forward the `supportShow` data to the switch supplier for further investigation.

I2C bus Errors

I2C bus errors indicate defective hardware, and the specific item is listed in the error message. Refer to the *HP StorageWorks Diagnostic and System Error Messages 4.2.x Reference Manual* for information specific to the error that was received. Specifically, some CPT and Environmental Monitor (EM) messages contain i2C-related information.

If the i2C message does not indicate the specific hardware that may be failing, begin debugging the hardware, as this is the most likely cause. The next sections provide procedures for debugging the hardware.

Check Fan Components

1. Log in to the switch as user.
2. Issue the `fanshow` command.
3. Check the fan status and speed output.

If any of the fan speeds display abnormal RPMs, replace the fan FRU.

Check the Switch Temperature

1. Log in to the switch as user.
2. Issue the `tempshow` command.
3. Check the temperature output.

Look for indications of high or low temperatures.

Check the Power Supply

1. Log in to the switch as user.
2. Issue the `psshow` command.
3. Check the power supply status. Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide*.

If a power supply shows a status other than OK, consider replacing it as soon as possible.

Check the Temperature, Fan, and Power Supply

1. Log in to the switch as user.
2. Issue the `sensorshow` command. Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for details regarding the sensor numbers.
3. Check the temperature output. Look for indications of high or low temperatures.
4. Check the fan speed output. If any of the fan speeds display abnormal RPMs, replace the fan FRU.
5. Check the Power Supply status. If a power supply shows a status other than OK, consider replacing it as soon as possible.

Device Login Issues

In narrowing down problems with device logins, use the following commands:

1. Log in to the switch.
2. Issue the `switchShow` command. Check for correct logins.

Example

```
switch:admin> switchshow
switchName:     switch
switchType:     16.2
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   7
switchId:       fffc07
switchWwn:      10:00:00:60:69:c0:0e:88
switchBeacon:   OFF
Zoning:         ON (cfg1)
port  0: id N2 Online       E-Port 10:00:00:60:69:c0:0f:04 "web189"
(upstream)

port  1: id N2 No_Light
port  2: id N2 No_Light
port  3: id N2 No_Light
port  4: id N2 No_Light
port  5: id N2 No_Light
port  6: id N2 No_Light
port  7: id N2 No_Light
switch:admin>
```

3. Issue the `portconfigShow` command to see how the port is configured.

Example

```
switch:admin> portcfgshow
Ports                  0  1  2  3    4  5  6  7
-------------------+--+--+--+--+----+--+--+--
Speed                 2G 2G 2G 2G   2G 2G 2G 2G
Trunk Port            .. .. ON ON   ON ON ON ON
Long Distance         .. .. .. ..   .. .. .. ..
VC link init          .. .. .. ..   .. .. .. ..
Locked L_Port         .. .. .. ..   .. .. .. ..
Locked G_Port         .. .. .. ..   .. .. .. ..
Disabled E_Port       .. .. .. ..   .. .. .. ..
Persistent Disable    .. .. .. ..   .. .. .. ..
ISL R_RDY Mode        .. .. .. ..   ON .. ON ..
                     where AN:AutoNegotiate, ..:OFF, ??:INVALID.
                            LM:L0.5
switch:admin>
```

4. Issue the `portErrShow` command. Check for errors that may cause login problems.
   - A high number of errors relative to the frames transmitted and frame received may indicate a marginal link. See "Marginal Links" on page 337.
   - A steadily increasing number of errors may indicate a problem. Track errors by sampling the port errors every five or ten seconds.

Example

```
switch:admin> porterrshow
frames enc crc too too bad enc disc link loss loss frjt fbsy
tx rx in err shrt long eof out c3 fail sync
sig==================================================================
===
0: 22 24 0 0 0 0 0 1.5m 0 7 3 0 0 0
1: 22 24 0 0 0 0 0 1.2m 0 7 3 0 0 0
2: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
3: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
4: 149m 99m 0 0 0 0 0 448 0 7 6 0 0 0
5: 149m 99m 0 0 0 0 0 395 0 7 6 0 0 0
6: 147m 99m 0 0 0 0 0 706 0 7 6 0 0 0
7: 150m 99m 0 0 0 0 0 160 0 7 5 0 0 0
8: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
9: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
10: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
11: 0 0 0 0 0 0 0 0 0 0 0 2 0 0
12: 0 0 0 0 0 0 0 0 0 0 0 2 0 0
13: 0 0 0 0 0 0 0 0 0 0 0 2 0 0
14: 0 0 0 0 0 0 0 0 0 0 0 2 0 0
15: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
32: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
33: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
34: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
35: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
36: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
37: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
38: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
39: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
40: 99m 146m 0 0 0 0 0 666 0 6 796 7 0 0
41: 99m 149m 0 0 0 0 0 15k 0 2 303 4 0 0
42: 99m 152m 0 0 0 0 0 665 0 2 221 5 0 0
43: 99m 147m 0 0 0 0 0 16k 0 2 144 4 0 0
44: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
45: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
46: 0 0 0 0 0 0 0 0 0 0 0 2 0 0
47: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

5. Issue the `portflagsshow` command to see how a port has logged in and where a login failed, if a failure occurred.

Example

```
 13: Online    In_Sync    PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED
CBL_LB L

OGIN LED

 14: Online    In_Sync    PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED
CBL_LB L

OGIN LED

 15: Online    In_Sync    PRESENT ACTIVE F_PORT L_PORT U_PORT LOGIN
NOELP LED AC

CEPT

 16: Online    In_Sync    PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED
CBL_LB L

OGIN LED
```

6. Issue the `portlogdump [count[, saved[, portid]]]` command. View the device-to-switch communication.

Example

```
switch:admin> portlogdump 41
time           task       event  port cmd  args
-------------------------------------------------
16:44:21.490   PORT        Rx      41   40
02fffffd,00fffffd,0005ffff,14000000
16:44:21.490   PORT        Tx      41    0  c0fffffd,00fffffd,00050541
16:44:32.503   PORT        Tx      41   40
02fffffd,00fffffd,0542ffff,14000000
16:44:32.506   PORT        Rx      41    0  c0fffffd,00fffffd,05420006
16:44:35.993   PORT        Rx       5   40
02fffffd,00fffffd,0a49ffff,14000000
16:44:35.993   PORT        Tx       5    0  c0fffffd,00fffffd,0a490543
16:44:35.997   PORT        Tx       5   40
02fffffd,00fffffd,0544ffff,14000000
16:44:36.000   PORT        Rx       5    0  c0fffffd,00fffffd,05440a4a
16:44:42.340   PORT        Rx      41   40
02fffffd,00fffffd,0009ffff,14000000
16:44:42.340   PORT        Tx      41    0  c0fffffd,00fffffd,00090545
switch:admin>
```

See Chapter 16, "Troubleshooting Using the Port Logs" on page 367 for information on decoding a `portlogdump`.

Firmwaredownload Issues (Core Switch 2/64 and SAN Director 2/128)

One indication that a firmware download sequence has failed is that a different version of firmware is running on each CP. Use the `firmwareshow` command to view the current firmware on each CP.

If a firmware download sequence has failed for any reason, use the following steps as an emergency recovery procedure.

1. Issue the `reboot` command to simultaneously reboot both the Active and the standby CPs.

2. Log in to a CP (either Active or Standby).
3. Issue the `firmwaredownload -s` command to download the desired firmware to a single CP.
4. Enter the user name and the Host IP (FTP server).
5. Choose the desired target firmware revision level.
6. Answer the prompts as they appear. The following are the recommended responses:
   - Answer `Y` (yes) to `Full Install`.

Note: Always answer `Y` to this prompt, unless directed otherwise by Technical Support. Answering no to this prompt can cause problems with the CP.

   - Answer `Y` (yes) to `Auto Commit` if you want the firmware to be committed automatically after download. If you answer `No`, you must manually issue the `firmwarecommit` command.

Example

```
switch: admin> firmwaredownload -s
Server Name or IP Address: 10.255.255.115
User Name:Admin
File Name: /pub/dist/system.plist
Password: xxxxxx
Full Install (Otherwise upgrade only) [Y]: n
Do Auto Commit after reboot [Y]: y
Reboot system after download [N]: N
```

7. Log in to the next CP.
8. Issue the `firmwaredownload -s` command to download the desired firmware to that single CP.
9. Enter the user name and the Host IP (FTP server).
10. Choose the desired target firmware revision level.
11. Answer the prompts as they appear. The following are the recommended responses:

- Answer `Y` (yes) to `Full Install`. Answering `No` to this prompt can cause problems with the CP.
- Answer `Y` (yes) to Auto Commit if you want the firmware to be committed automatically after download. If you answer no, you must manually issue the `firmwarecommit` command.

12. Issue the `reboot` command to simultaneously reboot both the Active and the standby CPs.

Watchdog (Best Practices)

Watchdog is a subset of the Kernel Error Reporting Software; it is a feature that reports unexpected and fatal errors when a switch dies. The Watchdog feature ensures that the switch does not send corrupted data when the software is not properly performing its function.

The ASIC has a Watchdog register that needs to be probed by the Fabric OS once every two seconds. If the ASIC detects that the Fabric OS is hung, the ASIC waits for an additional two seconds before resetting the CPU. The switch always reboots or fails over when a Watchdog error occurs.

Corrective Actions

In the event of a Watchdog error, perform the following steps:

- Collect the output of the `supportshow` command and contact Technical Support.
- (Optional and for FOS v2.x, v3.x) Turn on `settasklogmode` in the event of a Watchdog error; this allows more information to be collected. Do not enable this mode by default, since it slows traffic.
- See the specific error message for additional actions. See "Kernel Software Watchdog Related Errors" on page 320.

Kernel Software Watchdog Related Errors

This section explains kernel software watchdog error messages and provides corrective actions for each.

kSWD-APP_NOT_REFRESH_ERR

Message

```
Critical kSWD-APP_NOT_REFRESH_ERR, 1, (kSWD)Application with
pid <PID number> not refreshing watchdog.
```

Explanation A critical kernel software error occurred in the Watchdog subsystem. A kernel application is not able to refresh. See the specified PID number to find out which application is failing. The switch reboots (on single-CP switches) or fails over (on dual-CP switches).

Action Issue the `savecore` command to find if a Core File was created. If a Core File is found, select the `FTP the file` option.

Copy the error message and contact customer support.

Severity Critical

kSWD-kSWD_GENERIC_ERR_CRITICAL

Message

```
Critical kSWD-kSWD_GENERIC_ERR_CRITICAL, 1, kSWD: <error
string>
```

Explanation A critical application error was reported in the Watchdog subsystem. See the string at the end of the error message for specific information. The switch reboots (on single-CP switches) or fails over (on dual-CP switches).

Action Issue the `savecore` command to find out whether a Core File was created. If a Core File is found, select the `FTP the file` option.

Copy the error message and contact customer support.

Severity Critical

Identifying Media-Related Issues

Use the following section to narrow down media-related issues in the fabric.

Component Tests Overview

Hardware diagnostics available on switches can be classified into two different types of tests (Table 30 specifies the component tests):

- Structural tests perform basic tests of the switch circuit. When structural tests fail, replace the mainboard.
- Functional tests verify the intended operational behavior of the switch by running frames through ports or bypass circuitry.

Table 30: Component Test Descriptions

Test Name	Operands	Checks
crossporttest	[-nframes count] [-lb_mode mode][-spd_mode mode] [-gbic_mode mode] [-norestore mode] [-ports itemlist]	Functional test of port external transmit and receive path. The crossport is set to loopback using an external cable by default. However, this command can be used to check internal components by setting the lb operand to 5.
fporttest	[-nframes count] [-ports itemlist] [-seed payload_pattern] [-width pattern_width] [-size pattern_size]	Tests component to or from HBA. Used to test online F_Port devices, N_Port devices and SFPs/GBICs.
loopporttest	[-nframes count] [-ports itemlist][-seed payload_pattern] [-width pattern_width]	Only tests components attached to switch that are on a FC arbitrated loop.
spinfab	[nMillionFrames [, ePortBeg [, ePortEnd [, setFail]]]]	Tests components to or from a neighbor switch, such as ISLs and SFPs/GBICs between switches.

Check Switch Components

This section discusses the components of check switch and contains the following topics:

Cursory Debugging of Media Components

The following procedure describes basic steps that can help to narrow down faulty media.

1. Log in to the switch as admin.
2. Issue the `switchshow` command. Look for a known good portstate online or insync.
3. (Optional) Issue the `version` command. The version can be used to check the known buglist in the appropriate Release Notes.
4. Issue the `porterrshow` command. An error summary of all ports is displayed.
5. Glance over the port statistics.
   - Most numbers should be small. An excessively large number (such as one over 100,000) could indicate a bad transceiver.
   - Check for rapidly rising error counts.

Tip: The LLI_errs (Low Level Interrupt_errors) are the sum of the port's 8 statistical error counters: ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, and DiscC3. Check `porterrshow` output to determine what generated LLI_errs.

6. (Optional) Run tests if you still suspect a media problem.
   - To test components to and from a neighbor switch, see "Test Cascaded Switch ISL Links" on page 323.
   - To test a port's external transmit and receive path, see "Check a Port's External Transmit and Receive Path" on page 329.
   - To test the internal components of a suspect switch, see "Test a Switch's Internal Components" on page 325.
   - To test the components between a switch and a hub (and back), see "Test Components to and From the HBA" on page 326.
   - To check all switches attached components (on an FC loop), see "Check All Switch Components Between Main Board, SFP, and Fiber Cable" on page 326.
   - To check all of a port's attached components (on an FC loop), see "Check a Port's External Transmit and Receive Path" on page 329.
   - To view a list of additional component tests, see "Additional Component Tests" on page 331.

Test Cascaded Switch ISL Links

To test components to and from a neighbor switch:

1. Log in to the switch as admin.
2. Issue the `spinfab` command with the following operands (refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more details):
   - [`-nmegs` *`count`*] specifies the number of frames to send in millions
   - [`-ports` *`list`*] (optional) specifies a list of user ports to test
   - [`-setfail` *`mode`*] specifies a value of `1` to mark failing ports as BAD, specifies a value of `0` to not mark failed ports as bad
   - [`-domain` *`value`*] (optional) specifies a remote domain to which the switch is connected

Example

```
switch:admin> setdbg "DIAG", 0
switch:admin> spinfab 3,0,4

spinFab running...

spinFab: Completed 3 megs, status:  passed.
        port 0 test status: 0x00000000 --  passed.
        port 1 test status: 0x00000000 --  passed.
        port 2 test status: 0x00000000 --  passed.
        port 3 test status: 0x00000000 --  passed.
        port 4 test status: 0x02000000 --  SKIPPED!

switch:admin> setdbg "DIAG", 2
switch:admin> spinfab 3,0,3

spinFab running...
port  1 Rx  1 million frames.
port  0 Rx  1 million frames.
port  2 Rx  1 million frames.
port  3 Rx  1 million frames.
port  1 Rx  2 million frames.
port  0 Rx  2 million frames.
port  2 Rx  2 million frames.
port  3 Rx  2 million frames.
port  1 Rx  3 million frames.
port  0 Rx  3 million frames.
port  2 Rx  3 million frames.
port  3 Rx  3 million frames.

spinFab: Completed 3 megs, status:  passed.
        port 0 test status: 0x00000000 --  passed.
        port 1 test status: 0x00000000 --  passed.
        port 2 test status: 0x00000000 --  passed.
        port 3 test status: 0x00000000 --  passed.

switch:admin>
```

Test a Port's External Transmit and Receive Path

1. Log in to the switch as admin.
2. Connect the port you want to test to any other switch port with the cable you want to test.
3. Issue the `crossporttest` command with the any of the following operands:

Note: The following is a partial list. Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more information.

- `[-nframes` *`count`*`]` specifies the number of frames to send.
- `[-lb_mode` *`mode`*`]` specifies the loopback point for the test.
- `[-spd_mode` *`mode`*`]` specifies the speed mode for the test.
- `[-ports` *`itemlist`*`]` specifies a list of user ports to test.

Example

```
switch:admin> crossporttest
Running Cross Port Test .... passed.
```

Test a Switch's Internal Components

To use the `crossporttest` to test a switches internal components:

1. Log in to the switch as admin.
2. Connect the port you want to test to any other switch port with the cable you want to test.
3. Issue the `crossporttest -lb_mode 5` command.

   where `5` is the operand that causes the test to be run on the internal switch components.

   The following is a partial list. Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more information:

   - `[-nframes` *`count`*`]` specifies the number of frames to send
   - `[-lb_mode` *`mode`*`]` selects the loopback point for the test
   - `[-spd_mode` *`mode`*`]` selects the speed mode for the test

- [-ports *itemlist*] specifies a list of user ports to test

Test Components to and From the HBA

1. Log in to the switch as admin.
2. Issue the `fPortTest` command with the following operands (refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for details):
   - [*passCount*] specifies the number of times (or number of frames per port) to execute this test (default is infinite or until **Enter** key is pressed)
   - [*port_number*] specifies the port on which to run to test (F_Port by default)
   - [*payload_pattern*] specifies the pattern of the test packet payload
   - [*pattern_width*] specifies the width of the pattern which user specified - it could be 1, 2, or 4 (which are byte, word, or quad)
   - [*pattern_size*] specifies the number of words in test packet payload (default is 512)

   Example

```
switchname:admin> fporttest 100,8,0xaa55,2, 512
 Will use pattern: aa55  aa55  aa55 aa55  aa55  aa55 ...
 Running fPortTest ........
 port 8 test passed.
 value = 0
```

   The example above executed `fPortTest` 100 times on port 8 with the payload pattern 0xaa55, pattern width 2 (meaning word width) and default payload size 512 bytes.

Check All Switch Components Between Main Board, SFP, and Fiber Cable

The following procedure exercises all the switch components from the main board: SFP to fiber cable to SFP on the device, and back to main board.

1. Make sure all connected cables and SFPs are of the same technology (that is, a short wavelength SFP switch port should be connected to another short wavelength device SFP through a short wavelength cable).
2. Log in to the switch as admin.
3. Determine which ports are L-Ports by issuing the `switchshow` command.

4. Enable ports for loopback mode by issuing `loopporttest [--slot number] [-nframes count][-ports itemlist][-seed payload_pattern][-width pattern_width]`.

   Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more information about the operands.

5. Create a frame F of data size 1024 bytes.
6. Transmit frame F via port M, with D_ID to the FL port (AL_PA = 0).
7. Pick up the frame from port M, the FL port.
8. Determine whether any of the following statistic error counters are non-zero:

   ```
   ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out,
   BadOrdSet, DiscC3.
   ```

9. Determine whether the transmit, receive, or class 3 receiver counters are stuck at a value.
10. Determine whether the number of frames transmitted is not equal to the number of frames received.
11. Repeat step 5 through step 10 for all L-ports present until:
    - the number of frames requested is reached
    - all ports are marked bad
12. Look for errors. See the list below for possible errors.

Possible Errors

One or more of the following errors may appear if failures are detected. Refer to the *HP StorageWorks Diagnostic and System Error Messages 4.2.x Reference Manual* to find details and actions for any errors that appear.

```
DATA

INIT

PORT_DIED

EPI1_STATUS_ERR

ERR_STAT

ERR_STATS_2Long

ERR_STATS_BADEOF

ERR_STATS_BADOF
ERR_STATS_C3DISC

ERR_STATS_CRC

ERR_STATS_ENCIN

ERR_STATS_ENCOUT

ERR_STATS_TRUNC

ERR_STAT_2LONG

ERR_STAT_BADEOF

ERR_STAT_BADOS

ERR_STAT_C3DISC

ERR_STAT_CRC

ERR_STAT_ENCIN

ERR_STAT_ENCOUT

ERR_STAT_TRUNC

FDET_PERR

FINISH_MSG_ERR

FTPRT_STATUS_ERR

MBUF_STATE_ERR

MBUF_STATUS_ERR

NO_SEGMENT

PORT_ABSENT

PORT_ENABLE

PORT_M2M
```

```
PORT_STOPPED
PORT_WRONG
RXQ_FAM_PERR
RXQ_RAM_PERR
STATS
STATS_C3FRX
STATS_FTX
TIMEOUT
XMIT
```

Check a Port's External Transmit and Receive Path

The following procedure exercises the path of a loop from the port N transmitter, along the parallel loopback path, and back to the same N port transmitter. Loopback adapters are optional for this test.

This test does *not* exercise the SFP or the fiber cable. This test checks only components that are attached to the switch and that are on an FC arbitrated loop.

1. Log in as admin.
2. Disable the switch by issuing the `switchdisable` command.
3. Issue `portloopbacktest [`*`passcount`*`]` to set all ports for parallel loopback.

   Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for detailed information about the optional operand.
4. Transmit frame F through port N.
5. Pick up the frame from the same port N.
6. Check the following statistic error counters for non-zero values:

   ```
   ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_Out,
   BadOrdSet, DiscC3
   ```
7. Check whether the transmit, receive, or class 3 receiver counters are stuck at a value.
8. Check whether the number of frames transmitted is not equal to the number of frames received.
9. Repeat step 4 through step 8 for all ports present until:
   - The number of frames (or passCount) requested is reached.
   - All ports are marked as bad.

Possible Errors

One or more of the following errors may appear if failures are detected. Refer to the *HP StorageWorks Diagnostic and System Error Messages 4.2.x Reference Manual* to find details and actions for any errors that appear.

```
DIAG-INIT
DIAG-PORTDIED
DIAG_XMIT
DIAG-TIMEOUT
DIAG_ERRSTAT
DIAG-STATS
DIAG-DATA
```

Check Switch Components of the Port Transmit and Receive Path

The following procedure exercises all the switch components from the main board to SFP, to fiber cable, back to SFP, back to main board.

1. Make sure all cables used for connected ports and SFPs are of the same technology (that is, a short wavelength SFP switch port should be connected to another short wavelength device SPF through a short wavelength cable).
2. Connect ports from different ASICs, if possible (for example, connect port 1 - port 7).
3. Log in to the switch as admin.
4. Issue `switchdisable` if the switch should assume that all ports are cable loopbacked (and test accordingly).

   Or

   Leave the switch enabled if only cable loopbacked ports should be tested (and the rest ignored).
5. (Optional) Issue `setmediamode` to limit the test to ports that contain SFPs. This mode must be disabled when the test is complete.
6. Enable the ports for cabled loopback mode by issuing `crossporttest` with the selected operands.

   Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for details regarding the operands.
7. Create a frame F of maximum data size (2112 bytes).
8. Transmit frame F through port M.

9. Pick up the frame from its cross connected port N. An error is reported if any port other than N actually receives the frame.
10. Determine whether any of the following statistic error counters are non-zero:

    `ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3.`
11. Determine whether the transmit, receive, or class 3 receiver counters are stuck at a value.
12. Determine whether the number of frames transmitted is or is not equal to the number of frames received.
13. Repeat step 7 through step 12 for all ports until:
    - The number of frames requested is reached.
    - All ports are marked bad.
14. (Optional) Disable SFP mode. If `setmediamode` was entered, the mode remains in volatile memory until it is disabled. Issue `setmediamode 0`.

Additional Component Tests

Table 31 displays additional tests that can be used to determine those switch components that are not functioning properly. Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for details on these tests.

Table 31: Switch Component Tests

Test	Function
`portloopbacktest`	Functional test of port N->N path. See "Check a Port's External Transmit and Receive Path" on page 329.
`portregtest`	A read and write test of the ASIC SRAMs and registers.
`spinsilk`	Functional test of internal and external transmit and receive paths at full speed.
`sramretentiontest`	Verifies that data written into the miscellaneous SRAMs in the ASIC are retained after a 10 second wait.
`crossporttest`	Verifies the functional components of the switch.
`turboramtest`	Verifies the on chip SRAM located in the 2 Gbit/sec ASIC using the Turbo-Ram BIST circuitry. These same SRAMS are tested by `portregtest` and `sramretentiontest` using PCI operations, but for this test the BIST controller is able to perform the SRAM write and read operations at a much faster rate.

Table 31: Switch Component Tests (Continued)

Test	Function
`statstest`	Verifies the 2 Gbit/sec ASIC statistics counter logic.
Related Switch Test Command	
`itemlist`	Lists parameter syntax and grammar information; restricts the items to be tested to a smaller set of the parameter values.

Link Failure

A link failure occurs when a server or storage is connected to a switch, but the link between the server and storage, and the switch does not come up. This prevents the server and storage from communicating through the switch.

If the `switchshow` command or the LED lights indicate that the link has not come up properly, follow the steps for one or more of the areas indicated below.

A link failure can be caused by one of the following:

- "Switch State" on page 332
- "Port's Physical State" on page 333
- "Speed Negotiation Failure" on page 334
- "Link Initialization Failure (Loop)" on page 335
- "Port Has Come Up in a Wrong Mode" on page 336

Switch State

1. Issue the `switchshow` command.
2. Check the `switchState` entry in the `switchshow` command output.
3. Use Table 32 to determine the next step:

Table 32: SwitchState and Suggested Actions

SwitchState	Action
Online	The state of the switch is OK. Move on to check the "Port's Physical State" on page 333.
Offline	Enable the switch by issuing the `switchenable` command.
Testing	Wait for the switch to complete its test.
Faulty	Check the condition of the switch. Issue the `switchStatusShow` and `errShow` or `errDump` commands and identify the malfunctioning parts. Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more information.

Port's Physical State

1. Issue the `switchshow` command.
2. Check the port and state columns in the `switchshow` output.
3. Use Table 33 to determine the next step:

Table 33: Port States and Suggested Actions

Port State	Action
Online	The port physical state is OK. If the link has not come up, go to "Port Has Come Up in a Wrong Mode" on page 336.
No_Card	Check the SFP/GBIC.
No_Module	Check the SFP/GBIC.
No_Light	Check the physical contact and the cabling.
No_Sync	The port is receiving light but out of sync. Move on to "Speed Negotiation Failure" on page 334.
In_Sync	The port is in sync, but is not online. Move on to "Link Initialization Failure (Loop)" on page 335.
Laser_Flt	Check the physical contact and the cabling.
Port_Flt	Check the physical condition of the port. See "Identifying Media-Related Issues" on page 321.
Diag_Flt	Check the physical condition of the port. Issue the `diagShow` and `errShow` or `errDump` commands and identify the cause.
Testing	Wait for the completion of the test.

Speed Negotiation Failure

Note: Skip this section if the port speed is set to a static speed by the `portCfgSpeed` command.

The port negotiates the link speed with the opposite side. The negotiation usually completes in 1-2 seconds; however, sometimes the speed negotiation fails.

Determine if the negotiation was successfully completed:

1. Issue the `portLogShow` or `portLogDump` command.
2. Check the events area of the output for the following information:

   1 Gig example:

   ```
   14:38:51.976  SPEE       sn       <Port#>   NC
   00000001,00000000,00000001
   ```

   2 Gig example:

   ```
   14:39:39.227  SPEE       sn      <Port#>   NC
   00000002,00000000,00000001
   ```

   In the above examples:

   - The `sn` field indicates a speed negotiation.
   - The `NC` field indicates Negotiation Complete.
   - The `01` and `02` fields indicate the speed that has been negotiated.

   If these fields do not appear, move on to the step 3.
3. Correct the negotiation by issuing the `portCfgSpeed [`*`slotnumber`*`/]`*`portnumber`*`,` *`speed_level`* command if the fields above do not appear.

Link Initialization Failure (Loop)

1. Verify that the port is an L_Port.
   a. Issue the `switchShow` command.
   b. Check the comment field of the output to verify that the switch port indicates an L_Port. If a loop device is connected to the switch, the switch port must be initialized as an L_Port.
2. Verify the loop initialization *if* the port is not an L_port.
   a. Issue the `portLogShow` or `portLogDump` command.
   b. Check the event area for a `loopscn` entry with the `LOOP` command

   Example:

```
14:35:12.866   tReceive    loopscn   <Port#>   LOOP 10f5cbc0
```

   The loopscn entry display indicates that the loop initialization is complete. Do not perform a point-to-point initialization.

   HP StorageWorks switches the point-to-point initialization after the Loop Initialization Soft Assigned (LISA) phase of the loop initialization. This behavior sometimes causes trouble with old HBAs.

   If this is the case, skip the point-to-point initialization by issuing the `portCfgLport` command.

Point-to-Point Initialization Failure

1. Confirm that the port is active

   If a Fabric device or another switch is connected to the switch, the switch port must be active.
   a. Issue the `portLogShow` or `portLogDump` commands.
   b. Verify that the State Change Notification (SCN) code is 1. An SCN of 1 indicates that the port is active.

      Example:

```
13:25:12.506   PORT        scn       <Port#>    1
```

Do not perform the loop initialization phase. After becoming an active port, the port becomes an F_Port or an E_Port, depending on the device on the opposite side. If the opposite device is a Fabric device, the port becomes an F_Port. If the opposite device is another switch, the port becomes an E_Port.

Some Fabric devices have a problem with loop initialization. If this is the case, issue the `portCfgGport` command.

Port Has Come Up in a Wrong Mode

1. Issue the `switchShow` command.
2. Check the comment fields for the output in Table 34 and follow the suggested actions.

Table 34: SwitchShow Output and Suggested Action

Output	Suggested Action
Disabled	Issue the `portEnable` command.
Bypassed	Check the output from `portLogShow` or `portLogDump` commands and identify the link initialization stage where the initialization procedure went wrong.
Loopback	Check the output from `portLogShow` and `PortLogDump` commands and identify the link initialization stage where the initialization procedure went wrong.
E_port	If the opposite side is not another switch, the link has come up in a wrong mode. Check the output from `portLogShow/PortLogDump` commands and identify the link initialization stage where the initialization procedure went wrong.
F_port	If the opposite side of the link is a fabric device, the link has come up in a wrong mode. Check the output from `portLogShow` or `PortLogDump` commands.
G_port	The port has not come up as an E_port or F_port. Check the output from `portLogShow` or `PortLogDump` commands and identify the link initialization stage where the initialization procedure went wrong.
L_port	If the opposite side is *not* a loop device, the link has come up in a wrong mode. Check the output from `portLogShow` or `PortLogDump` commands and identify the link initialization stage where the initialization procedure went wrong.

Marginal Links

A marginal link involves the connection between the switch and the edge device. Isolating the exact cause of a marginal link involves analyzing and testing many of the components that make up the link: switch port, switch SFP, cable, the edge device, and the edge device SFP.

Confirming the Problem

The following steps provide a brief overview of possible steps to troubleshoot a marginal link.

1. Issue the `portErrShow` command. See the following output example.

Example

```
switch:admin> porterrshow
       frames  enc  crc  too  too  bad  enc disc link loss loss frjt fbsy
      tx    rx   in  err shrt long  eof  out   c3 fail sync sig
sig=================================================================
 0:   22   24    0    0    0    0    0 1.5m    0    7    3    0    0    0
 1:   22   24    0    0    0    0    0 1.2m    0    7    3    0    0    0
 2:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
 3:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
 4:  149m  99m   0    0    0    0    0  448    0    7    6    0    0    0
 5:  149m  99m   0    0    0    0    0  395    0    7    6    0    0    0
 6:  147m  99m   0    0    0    0    0  706    0    7    6    0    0    0
 7:  150m  99m   0    0    0    0    0  160    0    7    5    0    0    0
 8:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
 9:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
10:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
11:    0    0    0    0    0    0    0    0    0    0    0    2    0    0
12:    0    0    0    0    0    0    0    0    0    0    0    2    0    0
13:    0    0    0    0    0    0    0    0    0    0    0    2    0    0
14:    0    0    0    0    0    0    0    0    0    0    0    2    0    0
15:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
32:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
33:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
34:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
35:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
36:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
37:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
38:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
39:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
40:    99m 146m  0    0    0    0    0  666    0    6  796    7    0    0
41:    99m 149m  0    0    0    0    0  15k    0    2  303    4    0    0
42:    99m 152m  0    0    0    0    0  665    0    2  221    5    0    0
43:    99m 147m  0    0    0    0    0  16k    0    2  144    4    0    0
44:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
45:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
46:    0    0    0    0    0    0    0    0    0    0    0    2    0    0
47:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
switch:admin>
```

2. Establish whether there are a relatively high number of errors (such as CRC errors or ENC_OUT errors), or if there are a steadily increasing number of errors to confirm a marginal link.

Isolating the Areas

1. Move the suspected marginal port cable to a different port on the switch.
   - If the problem stops or goes away, the switch port or the SFP is marginal. Continue to step 2.
   - If the problem does *not* stop or go away, see "Ruling Out Cabling Issues" on page 339 or "Checking for Nx_Port (Host or Storage) Issues" on page 339.
2. Replace the SFP on the marginal port.
3. Issue the `portLoopBack` test on the marginal port. Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* or "I2C bus Errors" on page 311 for more information.
4. Check the results of the loopback test, and proceed as follows:
   - If the loopback test failed, the port is bad. Replace the port card.
   - If the loopback test did not fail, the SFP was bad.

Ruling Out Cabling Issues

1. Begin by performing the steps in "Isolating the Areas" on page 339.

   By now an SFP problem is ruled out.
2. Insert a new cable in to the suspected marginal port.
3. Issue the `portErrShow` command to determine if a problem still exists.
   - If the `portErrShow` output displays a normal number of generated errors, the issue is solved.
   - If the `portErrShow` output still displays a high number of generated errors, move on to "Checking for Nx_Port (Host or Storage) Issues" on page 339.

Checking for Nx_Port (Host or Storage) Issues

1. Begin by performing the steps in "Isolating the Areas" on page 339 and "Ruling Out Cabling Issues" on page 339. By now an SFP problem and a cable problem have been ruled out.
2. Follow the troubleshooting procedures for the Host or Storage device.

Switch Hangs when Connected to a Terminal Server

If a switch appears to be hung-up or passing no data (including error messages to the serial portLog), it may indicate that the switch is being Flow Controlled by a terminal server. By default, Flow Control is disabled on v3.1 and v4.2.x switches; however, if Flow Control has been enabled, it could cause a switch to hang.

Determining if a Switch is Being Flow Controlled

Flow Control is most likely causing a switch to hang if all of the following are true:

- A terminal server is connected to the serial port.
- The switch is not sending messages to the serial portLog.
- Flow Control has been enabled on the terminal server.

  If the statements above are true, Flow Control from the terminal server is most likely preventing the switch from passing traffic. See "Correcting a Hung Switch" on page 340 to correct the problem.

Correcting a Hung Switch

If Flow Control has been enabled, and a switch is being Flow Controlled by a terminal server, perform the following procedure:

1. Access the console.
2. Press **CTRL+Q** to cause the terminal to reenable flow.
3. Determine whether Flow Control is enabled, using the appropriate commands for the terminal server or terminal emulator.

> **Caution:** Though Flow Control may need to be disabled on the client device, disabling Flow Control *can* create a separate undesirable situation: unexpected or missing information in the serial portLog. See "Unexpected Output in the Serial PortLog" on page 341.

4. Disable Flow Control if it is enabled. Use of Flow Control can cause a switch to hang if it fails to manage the Flow Control properly, or manages it out of the expected sequence.

Unexpected Output in the Serial PortLog

Console serial port logs can sometimes appear to have incorrect, corrupt, or missing information due to potential overruns when connected to:

- Terminal emulation programs
- Terminal emulation devices
- Concentrators

If your serial port is connected to any of the hardware or software listed above, perform the following steps:

1. Determine whether your serial port is connected to terminal emulation/terminal servers/concentrators.
2. Access the console.
3. Determine whether Flow Control is disabled, using the appropriate commands for the device. Flow Control is disabled by default for v3.1.2 and v4.2.x.

   If Flow Control is disabled, this is most likely causing the incorrect data in the serial portLog.

Caution: Though Flow Control may need to be enabled on the client device, use of flow control *can* create a separate, undesirable situation. Flow Control may cause the switch to appear to hang if the client device fails to manage the flow control properly, or manages it out of the expected sequence. See "Switch Hangs when Connected to a Terminal Server" on page 340.

---

4. Enable Flow Control on the device.

   See "Switch Hangs when Connected to a Terminal Server" on page 340 for more Flow Control-related information.

Inaccurate Information in the Error Log

In rare instances, events gathered by the Track Change feature can report inaccurate information to the Error Log.

For information regarding enabling and disabling Track Changes (TC), see "Tracking Switch Changes" on page 77.

Scenario:

A user entered a correct user name and password, but the login was rejected because the maximum number of users had been reached. However, in the error log, the login was reported as successful.

Explanation:

If the maximum number of switch users has been reached, the switch still performs correctly in that it rejects the login of additional users (even if they enter the correct user name and password information).

However, in this limited scenario, the Track Change feature reports this event inaccurately to the Error Log; it appears that the login was successful. This scenario occurs only when the maximum number of users has been reached; otherwise, the login information displayed in the error log should reflect reality.

Troubleshooting Using the Port Logs

15

The portlogdump command output is a powerful tool that can be used to troubleshoot fabric issues. Use the portlogdump output and this chapter to read the actions and communications of a fabric. By understanding the processes that are taking place in the fabric, you can locate areas that may be problematic.

This chapter lists most of the Fibre Channel codes that you need to decode your Fibre Channel portlogdump traces and/or Fibre Channel analyzer traces, and explains how to decode the Fabric OS portlogdump traces.

Using the portlogdump Reference requires that you be familiar with the Fibre Channel Physical (PFC_PH) frame and the portlogdump format, and also understand the types of frames. The release version of this document correlates to the latest release version of the HP StorageWorks firmware.

Note: Information contained herein is subject to change without notice. In addition, undocumented messages may appear in the portlogdump.

This chapter discusses the following major topics:

Understanding the portlogdump Command

The `portlogdump` command displays the port log, showing a portion of the FC-PH header (see "The FC_PH Frame" on page 367) and the payload (see "Payload Information" on page 481).

Reading portlogdump Entries

Click on the links in example below to view information about that entry.

Example

```
RSL_SWT134:admin> portlogdump
Time Task Event Port Cmd Arguments
-------------------------------------------------
16:30:41.780  PORT       Rx       9   40  02fffffd,00fffffd,0061ffff,14000000
16:30:41.780  PORT       Tx       9    0  c0fffffd,00fffffd,0061030f
16:30:42.503  PORT       Tx       9   40  02fffffd,00fffffd,0310ffff,14000000
16:30:42.505  PORT       Rx       9    0  c0fffffd,00fffffd,03100062
16:31:00.464  PORT       Rx       9   20  02fffc01,00fffca0,0063ffff,01000000
16:31:00.464  PORT       Tx       9    0  c0fffca0,00fffc01,00630311
16:31:00.465  nsd        ctin     9   fc  000104a0,0000007f
16:31:00.465  nsd        ctout    9   fc  00038002,00000003,01fffc01
16:31:00.466  PORT       Tx       9  356  03fffca0,00fffc01,00630311,01000000
16:31:00.474  PORT       Rx       9    0  c0fffc01,00fffca0,00630311
16:31:01.844  PORT       Tx       9   40  02fffffd,00fffffd,0312ffff,14000000
16:31:01.854  PORT       Rx       9    0  c0fffffd,00fffffd,03120064
16:31:01.963  PORT       Rx       9   40  02fffffd,00fffffd,0065ffff,14000000
16:31:01.963  PORT       Tx       9    0  c0fffffd,00fffffd,00650313
16:31:14.726  INTR       pstate   0  LF2
16:31:14.729  PORT       scn      0  137  00000000,00000000,00000008
16:31:14.729  PORT       scn      0  129  00000000,00000000,00000400
16:31:14.729  PORT       scn      0    2  00010004,00000000,00000002
16:31:14.730  SPEE       sn       0   ws  00000002,00000000,00000000
<output truncated>
```

Additional portlogdump Examples

For more `portlogdump` examples, see:

- "Reading an SCN Event" on page 376
- "ELS Examples" on page 406

- "SW_ILS Examples" on page 414
  - "Routing Frame Example" on page 414
  - "NSD Example" on page 417
  - "SW_ILS Reject Example" on page 418
- "The ctin and ctout Event Examples" on page 471
- "Speed Negotiation Example" on page 398

Firmware Version Variations in the portlogdump

The following section described the major differences between the v3.x and v4.x `portlogdump` output.

Task Field Variations

The `portlogdump task` field has changed in v4.x. The Task field in v3.x displays a `t` before every task. In v4.x, the `t` no longer appears (see examples below).

Argument Field Variations

Fabric OS v3.x Example

In v3.x, the `args` field had 5 arguments. Argument 5 was an IU address pointer used by developers to obtain more data.

```
time            task    event  port  cmd   args
--------------------------------------------------
00:44:26.599    tFspf  Tx      8    40    02fffffd,00fffffd,0284ffff,14000000,10cac760
```

Fabric OS 4.x Example

In v4.x, there are a maximum of four arguments, and the *IU pointer* no longer appears (see examples).

```
time           task        event  port cmd args
--------------------------------------------------
16:30:41.780   PORT        Rx        9    40  02fffffd,00fffffd,0061ffff,14000000
```

Note the differences between the `task` column and the `args` columns from v3.x to 4.x.

Using and Customizing the portlogdump

There are several commands that can be used to view certain aspects of the `portlogdump` (such as a list of possible events), and to customize the output of the `portlogdump`.

Refer to the *HP StorageWorks Fabric OS 4.2.x Command Reference Guide* for more detailed command information.

Commands Related to portlogdump

The commands in Table 35 are related to the `portlogdump`.

Table 35: Commands Related to portlogdump

Command	Action
`portlogdump [`*`count`*`[, `*`saved`*`[, `*`portid`*`]]]`	Displays the port log, listing all entries in the log without page breaks. This command displays the same information as `portlogshow`, but `portlogshow` prompts you to press **Enter** between each page.
`portlogdumpport` *`portid`*	Displays the port log of specified port. The command displays all entries in the log without page breaks. It is identical to `portlogshow`, except that `portlogshow` prompts the user to press **Enter** between each page of output.
`portlogshow [`*`count, saved, portid`*`]`	Displays the port log. This command displays 22 entries at a time. The `portlogshow` command displays the same information as `portlogdump`, but it enables you to press **Enter** after each page of output.
`portlogclear`	Clears the port log. You may want to clear the port log before triggering an activity, so that the log displays only the activity related to that activity.
`portlogshowport [`*`portid`*`]`	Displays the port log of a specified port, showing 22 entries at a time. It is identical to `portlogdump`, except that `portlogdump` does not prompt the user to press **Enter** between each page of output.
`portlogtypedisable` *`type`*	Disables the port log for a specified port log type. Disabling the port log type prevents it from appearing in the `portlogdump` output.
`portlogtypeenable` *`type`*	Enables the port log for a specified port log type. Enabling the port log type allows it to appear in the `portlogdump` output.

Displaying a List of Possible Port Log Events

Use the following procedure to list port log events, and to find their associated ID number.

1. Log in to the switch as admin.
2. Issue the `portlogeventshow` command.
   - The left column displays the ID associated with the event. This number can be used to enable and disable an event; this keeps it from appearing in the `portlogdump` output.
   - The middle column displays the events.
   - The right column displays the enabled or disabled status of the event. A disabled event does not appear in the `portlogdump`. `0` = enabled, `1` = disabled.

Example

```
switch:admin> portlogeventshow
ID Event-Name   Disabled
---------------------------------
1   start          0
2   disable        0
3   enable         0
4   ioctl          0
5   Tx             0
6   Tx1            0
7   Tx2            0
8   Tx3            0
9   Rx             0
10  Rx1            0
11  Rx2            0
12  Rx3            0
13  stats          0
14  scn            0
15  pstate         0
16  reject         0
17  busy           0
18  ctin           0
19  ctout          0
20  errlog         0
21  loopscn        0
22  create         0
23  debug          1
24  nbrfsm         0
25  timer          0
26  sn             0
27  fcin           0
28  fcout          0
29  read           0
30  write          0
31  err            0
32  frame          0
33  msRemQ         0
34  msRemR         0
35  nsRemQ         0
36  nsRemR         0
37  rscn           0
38  state          0
39  xalloc         0
40  xfree          0
```

Customizing the portlogdump Output

1. Log in to the switch as admin.
2. Issue the `portlogeventshow` command.
   - The left column displays the ID associated with the event. Note the number of the specific event that you want to enable or disable.
   - The middle column displays the events.
   - The right column displays the enabled or disabled status of the event. A disabled event does not appear in the `portlogdump`. `0` = enabled, `1` = disabled.
3. Issue one of the following commands:

   `portlogtypeenable` *`type`* to enable the particular Event in the `portlogdump` output.

   Or

   `portlogtypedisable` *`type`* to disable the particular Event in the `portlogdump` output.

   Type is the ID Number gathered in step 2.

Example

```
switch:admin> portlogeventshow
ID Event-Name   Disabled
---------------------------------
1   start         1
2   disable       0
3   enable        0
4   ioctl         0
5   Tx            0
6   Tx1           0
7   Tx2           0
8   Tx3           0
9   Rx            0
10  Rx1           0
11  Rx2           0
12  Rx3           0
13  stats         0
14  scn           0
15  pstate        0
16  reject        0
17  busy          0
18  ctin          0
19  ctout         0
20  errlog        0
21  loopscn       0
22  create        0
23  debug         1
24  nbrfsm        0
25  timer         0
26  sn            0
27  fcin          0
28  fcout         0
29  read          0
30  write         0
31  err           0
32  frame         0
33  msRemQ        0
34  msRemR        0
35  nsRemQ        0
36  nsRemR        0
37  rscn          0
38  state         0
39  xalloc        0
40  xfree         0
switch:admin> portlogtypedisable 1
```

In the example above, the start event is disabled. It does not appear in the `portlogdump` output.

Locating Information by Task

Table 36 is an information map, and displays where to locate specific `portlogdump` information.

Table 36: Command portlogdump Information Mapping Table

Task	Event	Port	Command	Argument	Go to Page
tFabric	RSCN	Switch ID	N/A	N/A	page 376
	enable	Port #	1 = enable 2 = disable	IU pointer, 0	page 359
	ioctl	Port #	IOCTL code	IU pointer, 0	page 388
	pstate	Port #	Port State Machine	N/A	page 505
	Tx( )	Port #	Size of payload in bytes	Header & Payload If FC-CT (cmd) code	ELS / R_CTL=22/23: page 399 FC-CT/R_CTL=02/03
tFCP	Tx( )	Port #	Size of payload in bytes	Header & Payload	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02
	tFSPF ioctl	Port #			ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02
tFCPH	loopscn	Port #	Loopscan code	N/A	page 382
tFSPF	ioctl	Port #	IOCTL code	IU pointer, 0	page 388
	Tx( )	Port #	Size of payload in bytes	If FC-CT cmd code	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02
tInterrupt	pstate	Port #	Port State Machine Code	N/A	
	scn	Port #	Internal SCN Value	sn	
	scn	Port #	SW	Speed negotiation code	page 386
tLOOP	loopscn	Port #	LIP	Loop code	page 382

Table 36: Command portlogdump Information Mapping Table (Continued)

Task	Event	Port	Command	Argument	Go to Page
tMSd	Tx	Port #	Size of payload in bytes	If FC-CT cmd code	ELS / R_CTL=22/23: page 399 If FC-CTR_CTL=02
	ctin	Port #	CT_Type	FC_CT's payload	page 436
	Ctout	Port #		FC_CT's payload	page 436
tNSCAM	nsRemR	Port #	FCCT response code	Word0, word1, nameserver port type, IU pointer	page 436
	nsRemQ	Port #	Fabric Internal FC-CT command	Word0, word1, nameserver port type, IU pointer	page 436
	rscn	Port #	Request ID (24 bit addresses)	N/A	page 436
	ioctl	Port #	IOCTL code	pointer, 1	page 388
	tx	Port #	Size of payload in bytes	N/A	page 436
tNsd	ctin	Port #	Last byte of well known address	FC_CT's payload	page 436
	ctout	Port #	Last byte of well known address	FC_CT's payload	page 436
	nsRemR	Port #	FC_CT's payload	Word0, word1, nameserver port type, IU pointer	page 436
	sRemQ	Port #	Fabric Internal FC-CT command	Word0, word1, nameserver port type, IU pointer	page 436
	rscn	Port #	Request ID (24 bit FC addresses)	00fffffd, ELS code, IU pointers, IU pointer	ELS / R_CTL=22/23: page 399 If FC-CTR_CTL=02
	Tx( )	Port #	Size of payload in bytes	Word0, word1, nameserver port type, IU pointer	ELS / R_CTL=22/23: page 399 If FC-CTR_CTL=02
	create	null	null	tNSCAM	page 436

Table 36: Command portlogdump Information Mapping Table (Continued)

Task	Event	Port	Command	Argument	Go to Page
tReceive	Busy	Port #	Busy Reason Code	01 PHYSICAL_N_PORT_BUSY 03 N_PORT_RESOURCE_BUSY	
	disable	Port #	1 = enable, 2 = disable	N/A	page 359
	ioctl	Port #	IOCTL code	N/A	page 388
	loopscn	Port #	Loopscan code	N/A	page 382
	pstate	Port #	Port State Machine Code	LLI	page 505
	reject	Port #	null	Reject reason code page 411	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02: page 437
	Rx( )	Port #	Size of payload in bytes	If FC-CT cmd code. Also check R_CTL on page 368	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02: page 437
	scn	Port #	SCN Code.	Null	
	Tx( )	Port #	Size of payload in bytes	If FC-CT cmd code	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02: page 437
	sn	Port #	NC	Speed negotiation code,00000000,00000000	page 386
tResponse	Tx( )	Port #	Size of payload in bytes	If FC-CT cmd code	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02: page 437
tRT	Tx	Port #	Size of payload in bytes	ILS command code	page 409

Table 36: Command portlogdump Information Mapping Table (Continued)

Task	Event	Port	Command	Argument	Go to Page
tRtwr	debug	255		Respond IU, sent IU	
	Tx	Port #	Size of payload in bytes	Respond IU, sent IU	
tShell	Tx( )	Port #	Size of payload in bytes	If FC-CT cmd code	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02: page 437
	ioctl	Port #	Ioctl code	UI pointer, 0	page 388
	sn	Port	Name	State value	page 386
tSnmpd	create		null	tFaScn	page 359
SPEE	sn	Port #	WS	Speed negotiation event,00000000,0 0000000	page 386
tSwitch	ioctl	Port #	Ioctl code	N/A	page 388
	pstate	Port #	Port State Machine	N/A	page 505
	sn	Port #	WS	Speed negotiation event,00000000,0 0000000	page 386
	Tx( )	Port #	Size of payload in bytes	If FC-CT cmd code	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02: page 437
tTransmit	Reconf	Port #	BF (build fabric)	SW_ILS command codes	page 485
	ctin	Port #	Size of payload	FC-CT payload	page 437
	ctout	Port #	Size of payload	FC-CT payload	page 437
	Ioctl	Port #	IOCTL code		page 388

Table 36: Command portlogdump Information Mapping Table (Continued)

Task	Event	Port	Command	Argument	Go to Page
tZone	Ioctl	Port #	IOCTL code	IU pointer, IU pointer	page 388
	Reject	Port #	Reject	Reject code on page 411	page 423
	Tx( )	Port #	Size of payload in bytes	If FC-CT cmd code	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02: page 437
	Rx( )	Port #	Size of payload in bytes	If FC-CT cmd code	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02: page 437
PORT	ioctl	port#	IOCTL Code		page 388
	scn	port#	SCN Code	Null	page 375
	Tx ( )	port#	SCN Code	Size of payload in bytes	page 375
	Rx ( )	port#	Size of payload in bytes	If FC-CT cmd code	ELS / R_CTL=22/23: page 399 If FC-CT/R_CTL=02: page 437
INTR	PS (primitive sequence) pstate	port#	State Machine Value		page 505
FLTR	debug	Port#	NA	Internal debug codes	debug
LOOP	loopscn	Port#	Loopscan code - HP ASIC LOOP Code cmd column	HP ASIC LOOP Code LoopSCN Reason Code column	page 382

Table 36: Command portlogdump Information Mapping Table (Continued)

Task	Event	Port	Command	Argument	Go to Page
nsd	ctin	Port#	Last byte of well known address	FC_CT's payload	page 437
	ctout	Port#	Last byte of well known address	FC_CT's payload	page 437
	rscn	0	Word 0 = Domain Controller on another switch (Ex. fffcDD, where DD = Domain)	Word 1 = Domain Controller of switch passing change information, HP-specific command code for SW_ILS, Word 6, last 3 bytes = 24 bit address of changed devices	ELS Command Codes
	Rscn	0	Word 0 = 24 bit address device that did SCR	Word 1 = Domain Controller of switch passing change information, ELS Word 6, last 3 bytes = 24 bit address of changed device	ELS Command Codes
	nsRemQ	0: 1st nibble NS cmd code	Last 3 nibbles: Name Server Cmd code. Fabric internal FC-CT cmd codes	D_ID, S_ID, Name Server Port Type	page 437
	NsRemR	Port#	Name Server Cmd Code page 441	D_ID, S_ID, Additional information command code	page 437
msd	ctin	Port#	Last byte of well known address	FC-CT's payload	page 437
	ctout	Port#	Last byte of well known address	FC-CT's payload	page 437

Table 36: Command portlogdump Information Mapping Table (Continued)

Task	Event	Port	Command	Argument	Go to Page
FSS	msg	N/A		Service ID, Component ID, Send receive data, optional flags, Additional text description.	page 428
	cmd	N/A			page 428
	event	N/A			page 428

About the portlogdump Fields

This section discusses the following `portlogdump` fields:

- "Time" on page 359
- "Task" on page 359
- "Event" on page 362
- "Port" on page 364
- "Cmd" on page 364
- "Arguments" on page 365

Time

Time is the Event's date and time in milliseconds.

Example

```
16:30:41.780  PORT       Rx       9   40  02fffffd,00fffffd,0061ffff,14000000
16:30:41.780  PORT        Tx       9    0   c0fffffd,00fffffd,0061030f
16:30:42.503  PORT       Tx       9   40  02fffffd,00fffffd,0310ffff,14000000
```

Task

The Task column narrows the area being described by a specific line in the output.

Example

```
portlogdump:
time           task       event  port cmd  args
-------------------------------------------------
15:48:11.473  INTR       pstate  19  LF2
15:48:11.474  INTR       pstate  19  LF1
15:48:11.474  INTR       pstate  19  OL2
15:48:11.474  INTR       pstate  19  LR2
15:48:11.474  INTR       pstate  19  LR3
15:48:11.474  INTR       pstate  19   AC
15:48:11.474  PORT       scn     19   11  00000000,00000000,00010000
```

Task Descriptions

Table 37 lists the Tasks description and functionality.

Table 37: Task Descriptions

Task	Description	Function
v3.x Tasks		
tASd	Alias Server Daemon	The Alias service is used for managing multicast groups by supporting the create, add, remove, and destroy functions.
tErrlog	Error Log	Information fed into the error log task can be viewed using `errShow` and `Dump` commands.
tFabric	Fabric	Fabric initialization. Fabric configuration. FC-SW protocol - ELP, EFP.
tFaScn	Fabric Assist State Change Notification	Refers to Fabric Assist updates and changes. See "State Change Notification (SCN)" on page 375.
tFCP	Fibre Channel Protocol	Probe - query SCSI command.
tFCPH	Fibre Channel Physical	Handles frame sequences for FC-2 processes Frame at FC-2 level and below.
tFCPth		Monitors SCSI static components in Fabric.
tFspf	Fibre Channel Shortest Path First	Routing.
tHttpD	Web Server Daemon	Monitors the Web Server.
tInterrupt	Interrupt	See event associated with interrupt to identify the interrupt reason.
tMsApi	Management Server Application Programming Interface	Allows API calls into the switch for management and monitoring purposes.
tMSd	Management Server Daemon	Monitors the MS - includes the Fabric Configuration Service and the Unzoned Name Server.
tNSCAM	Name Server Cache Manager.	Updates the Name Server (NS) data bases across switches as a background task.
tNsd	Name Server Daemon	Monitors Name Server.
tReceive	Receive	Handles all frames received.
tResponse	Response	Sequence of the initiate.
TRestart	Restart	Task reboots system after stopping all activity.
tRlogind	Remote login daemon	Remote Login Information.

Table 37: Task Descriptions (Continued)

Task	Description	Function
tRt	Reliable Transport	Events we want to deliver but we do not care how long they take, such as, zoning delta propagation - persistently retries transmission of changed information to another switch.
tRtwr	Reliable Transport With Response	
tSnmpd	SNMP Agent Daemon	Monitors static components in Fabric.
tShell	Telnet	A Telnet task that starts up a shell in VX works.
tSwitch	Switch	First task started to control switch like a "parent" task. Major function includes initializing Mac address.
tSyslog	Syslog daemon	Used to forward error messages.
Task	Description	Functionality.
tThad	Threshold	Monitors static components in fabric.
tTimers	Timer	Time Out functions.
tThFru	Threshold Field Replaceable Unit	An FW task that monitors physical FRU components in fabric.It comes as a default whether or not the FW license exists.
tTransmit	Transmits	Sequences switch initiates.
v4.x Specific Tasks		
INTR	Internal	Events associated with this task: Port State (PS), and Debug.
PORT	Port kernel driver	Equivalent to "tReceive" and "tTransmit" in v3.x code, as well as any frame transmit of receive on behalf of any user processes (daemons). Events associated with task: debug, I/O control, State Change Notification, Transmit and Receive.
SPEED	Speed	ASIC speed negotiation function; speed selection between 1 or 2 Gbps.
FLTR	Filtering	ASIC frame filtering function; used in WWN zoning (WWN).
LOOP	Loop	ASIC loop function; it has to do with loop port initialization.
nsd	Name Server Daemon	NS daemon; same as tNSd for v3.x.

Table 37: Task Descriptions (Continued)

Task	Description	Function
msd	Management Server Daemon	MS daemon; same as tMSd for v3.x.
asd	Alias Server Daemon	AS daemon; same as tASd for v3.x. Events associated with this task: ctin and ctout.
fspfd	Fibre Channel Shortest Path First	Event associated with this task: Neighbor state transition.
zone	Zoning	Event associated with this task: debug.
fcpd	N/A	No event is associated with this task.
FSS	Fabric OS State Synchronization.	The primary function of FSS is to deliver State Update messages from ACTIVE components to their peer STANDBY components. FSS determines if fabric elements are synchronized (and thus FSS "compliant"). Associated events are: upconn, downconn, comp, incomp, dumprdy, syncsucc, failsync, start, stop, recovfail, take, yield, miscatch, update, active, standby, txqhigh, rxqhigh, misssvc, availsvc, trace.

Event

An Event is the specific action that is described by the output. For a complete list of possible events for your switch, see "Displaying a List of Possible Port Log Events" on page 348.

Example

```
portlogdump:
time           task       event  port cmd  args
-------------------------------------------------
15:48:11.473  INTR       pstate   19   LF2
15:48:11.474  INTR       pstate   19   LF1
15:48:11.474  INTR       pstate   19   OL2
15:48:11.474  INTR       pstate   19   LR2
15:48:11.474  INTR       pstate   19   LR3
15:48:11.474  INTR       pstate   19    AC
15:48:11.474  PORT       scn      19   11  00000000,00000000,00010000
```

The example above indicates that an internal task (INTR) --> associated event is the Port State Machine (pstate) --> and the **cmd** field describes the event, which is a link failure (LF2).

Events Descriptions

The following table describes the possible Events:

Table 38: Event Descriptions

Event	Description
start	Describes a switch start or restart event.
disable	Indicates a port is disabled.
enable	Indicates a port is enabled.
ioctl	Indicates a port I/O control is executed.
Tx	Indicates a frame is transmitted.
Tx()	Indicates a frame is transmitted, class 1, 2 or 3.
Rx	Indicates a frame is received.
Rx()	Indicates a frame is transmitted, class 1, 2 or 3.
stats	Indicates a port status or statistics.
scn	Indicates a state change notification.
pstate	Indicates a port changes physical state.
reject	Indicates a frame is rejected.
busy	Indicates a received frame is busied.
ctin	Indicates a Common Transport (CT)-based request is received.
ctout	Indicates a Common Transport (CT)-based response is transmitted.
errlog	Indicates a message is added to the error log.
loopscn	Indicates a loop state change notification.
create	Indicates a task is created.
debug	Indicates generic debugging information.
nbrfsm	Indicates a neighbor state transition.
timer	Indicates a timer.
sn	Indicates a speed negotiation.

Table 38: Event Descriptions (Continued)

Event	Description
nsRemQ	Indicates an inter-sw NS query.
nsRemR	Indicates an inter-sw NS response.
rscn	Indicates a Registered State Change Notification (RSCN).
Reconf	Indicates a fabric reconfiguration.
Debug	Indicates generic debugging information.
ps	Indicates a primitive sequence - used to denote pstates.

Port

The **port** field in the `portlogdump` output indicates a physical port number.

```
Nov 25        task       event port  cmd  args
----------------------------------------------
11:00:48.433  tReceive   Rx      12   40 02fffffd,00fffffd,00dbffff,14000000,11cd35a0
11:00:48.449  tTransmit  Tx      12    0  c0fffffd,00fffffd,00db0189,        ,11cd35a0
11:00:48.649  tReceive   Rx3      5  116 22240300,00140500,07acffff,03000000,11cd35a0
11:00:48.649  tTransmit  Tx3      2  116 22240300,00140500,07acffff,03000000,11cd35a0
11:00:49.166  tReceive   Rx3      2  116 221500ef,17240300,0095ffff,03000000,11cd7480
11:00:49.166  tReceive    reject   2        3
11:00:49.733  tFspf      Tx       2   40 02fffffd,00fffffd,018affff,14000000,11cdc090
```

Cmd

The **cmd** field represents different values, depending on the task and event.

Commands (`cmd`) are associated with each event category. For example, in the output below, the last line of the `cmd` column represents the scn code. If the event is an rx or PORT the `cmd` is usually the size of the payload.

```
portlogdump:
time           task       event  port cmd  args
-------------------------------------------------
15:48:11.473  INTR       pstate  19  LF2
15:48:11.474  INTR       pstate  19  LF1
15:48:11.474  INTR       pstate  19  OL2
15:48:11.474  INTR       pstate  19  LR2
15:48:11.474  INTR       pstate  19  LR3
15:48:11.474  INTR       pstate  19   AC
15:48:11.474  PORT       scn     19   11  00000000,00000000,00010000
```

Example State Events

Some possible State Events are:

- AC Active State
- FC Name Server (in MS)
- LR1 Link Reset: LR Transmit State
- LR2 Link Reset: LR Receive State
- LR3 Link Reset: LRR Receive State
- LF1 Link Failure: NOS Transmit State
- LF2 Link Failure: NOS Receive State
- OL1 Offline: OLS Transmit State
- OL2 Offline: OLS Receive State
- OL3 Offline: Wait for OLS State

Also see "ASIC Loop Codes" on page 382.

Arguments

The **args** field represents different values, depending on the task and event.

Example

```
time          task        event   port cmd args
-------------------------------------------------
11:01:15.166  tNSCAM      nsRemQ   0   4a0  00fffc24,00fffc14,0000007f,00000000
11:01:15.166  tNSCAM     Tx       2     4 02fffc24,00fffc14,01adffff,0000007f,11cdde40
11:01:15.183  tReceive   Rx       2   132 03fffc14,00fffc24,01ad032b,01000000,11cd35a0
11:01:15.183  tTransmit  Tx       2     0  c0fffc24,00fffc14,01ad032b,        ,11cd35a0
```

For more information regarding reading arguments, see "Reading portlogdump Entries" on page 345.

About Arguments in Older Firmware Versions

Firmware v2.x or Earlier

Prior to v2.1.2 firmware, the `portlogdump` format displayed only three arguments in the **args** field. The first two arguments belong to the FC_PH header (WD0 and WD1). The third argument belongs to the payload (WD6).

Firmware v2.x or Later

For firmware later than v2.1.2, but earlier than v3.0, the `portlogdump` format displays four arguments in the **args** field. The first three arguments belong to the FC_PH header (WD0,WD1, and WD4). The fourth argument belongs to the payload.

Firmware v3.x

Firmware v3.0 or greater displays five arguments in the **args** field. The fifth argument is an IU (Information Unit) address pointer. The undocumented command `iuShow` [0xIU pointer] provides more information about the frame. IU is the memory allocation, thus it can be taken by another task. Developers use this UI pointer for the reference to gather more information.

Firmware v4.x

In most instances, the IU pointer (the fifth argument, which is available in 3.x), does *not* appear in the v4.x firmware output.

In specific Tasks (such as FSS), a fifth argument is displayed; however, the display is in text instead of ASCII.

About the IU Pointer

The IU address pointer appears in the fifth argument of the `portlogdump` (for example, `10ca5ae0`) in versions prior to v4.x. Developers use this pointer to get more information. If the address is still available, issue `iuShow` 0xiupointer (to obtain more data). The IU pointer (the fifth argument) does not appear in the `portlogdump` of v4.x firmware.

The FC_PH Frame

About FC_PH Frames

For general Fibre Channel information, see "Fibre Channel Protocol Information" on page 502.

A Fibre Channel frame has a header and a payload (see Table 39). The header contains control and addressing information associated with the frame. The payload contains the information being transported by the frame and is determined by the higher-level service or FC_4 upper level protocol. There are many different payload formats based on the protocol (see Table 40).

- The TYPE field (Word2, bits 31-24) tells which information unit (IU) format to use.
- The routing control INFO bits (bit 27-24) determines how to interpret the payload.

Table 39: FC_PH Frame Diagram

4	8	Up to 2112 Bytes	4	4
S O F	HEADER	PAYLOAD	C R C	E O P

Table 40: FC_PH Frame Cross-References

	Word	Bits 31 - 24	Bits 23 - 16	Bits 15 - 8	Bits 7 - 0
HEADER	0	"Routing Control Bits (R_CTL)" on page 368	"Destination_ID (D_ID)" on page 370		
	1	"Class Specific Control Field (CS_CTL)" on page 374	"Sequence ID (SEQ_ID)" on page 372		
	2	"Type Code" on page 373	Frame Control (F_CTL), page 371		
	3	"Sequence ID (SEQ_ID)" on page 372	Data Field Control (DF_CTL), page 374	"Sequence Count (SEQ_CNT)" on page 372	
	4	"Originator ID (OX_ID)" on page 372		"Responder ID (RX_ID)" on page 372	
	5	Parameter			
	Payload - 6 to N word				

FC_PH Frame Definitions

Routing Control Bits (R_CTL)

Routing Control bits (R_CTL) are the first 8 bits of the header (see Table 41). They define the type of frame and its contents. The first four bits (bit 31-28) identify the frame type. The second four bits are the INFO bits (27-24); they define the contents of the frame or identify the function of the frame

Example

```
00:44:26.599  tFspf  Tx  8   40  02fffffd,00fffffd,0284ffff,14000000,10cac760
```

02 = R_CTL request

Table 41: Routing Control Bits - R_CTL Diagram

R_CTL Information		
R_CTL		
R_bits	Information	Description
FC-4 Device Data x'0'	0	Uncategorized Device Data
	1	Solicited Device Data
	2	Unsolicited Control Info (Request)
	3	Solicited Control Info (Reply)
	4	Unsolicited Device Data
	5	Data Descriptor
	6	Unsolicited Command
	7	Command Status Information
Extended Link Service x'2'	2	Request
	3	Reply
FC-4 Link Data x'3'	2	Request
Note - Same as FC-4 Device Data frames	3	Reply
	4	Video Data
Basic Link Service x'8'	0	No Operation (NOP)
	1	Abort Sequence (ABTS)
	2	Remove Connection (RMC)
	3	Reserved
	4	Basic_Accept (BA_ACC)
	5	Basic Reject (BA_RJT)
	6	Preempted (PRMT)
	Others	Reserved

Table 41: Routing Control Bits - R_CTL Diagram (Continued)

R_CTL Information		
Link Control x'C'	0	ACK
	1	ACK
	2	N_Port Reject (P_RJT)
	3	Fabric Reject (F_RJT)
	4	N_Port Busy (P_BSY)
	5	Fabric Busy to Data Frame (F_BSY)
	6	Fabric Busy to Link_Control Frame (F_BSY)
	7	Link Credit Reset (LCR)
	8	Notify (NTY)
	9	End
	Others	Reserved

Destination_ID (D_ID)

The Destination ID (D_ID) refers to the Native port address (24 bit address).

Example The `fffffd` field is the D_ID

```
00:44:26.599  tFspf  Tx  8   40  02fffffd,00fffffd,0284ffff,14000000,10cac760
```

In the example above, the D_ID is the Well Known Address of a Fabric Controller. See “Well-Known Addresses” on page 506 for a list of all Well Known Addresses.

Source_ID (S_ID)

The Source ID (S_ID) refers to the Native port address (24 bit address).

Example The `fffffd` field is the S_ID

```
00:44:26.599  tFspf  Tx  8   40  02fffffd,00fffffd,0284ffff,14000000,10cac760
```

In the example above, the S_ID is the Well Known Address of a Fabric Controller. See “Well-Known Addresses” on page 506 for a list of all Well Known Addresses.

Frame Control (F_CTL)

This field contains miscellaneous control information regarding the frame (see Table 42).

Table 42: Frame Control (F_CTL) Diagram

Frame Control Field Bits (F_CTL)		
Hex	Abbreviation	Description
0xC00000	FCTL_XCHSEQ	Exch & Seq Context bit mask
0x800000	FCTL_RESPXCH	Responder of Exchange
0x400000	FCTL_RECSEQ	Sequence Recipient
0x200000	FCTL_1STSEQ	First sequence of Exchange
0x100000	FCTL_LASTSEQ	Last sequence of Exchange
0x080000	FCTL_ENDSEQ	Last data frame of sequence
0x040000	FCTL_ENDCONN	End of Connection pending
0x020000	FCTL_CHAINEDSEQ	Chained Sequence active
0x010000	FCTL_SEQINIT	Transfer sequence initiative
0x800000	FCTL_NEWXID	X_ID reassigned
0x004000	FCTL_INVXID	Invalidate X_ID
0x003000	FCTL_ACKFORM	Ack form capability
0x000800	FCTL_COMPRESS	Data compression
0x000400	FCTL_ENCRYPT	Data encryption
0x000200	FCTL_RETXSEQ	Sequence retransmission
0x000100	FCTL_UNIDIRECTX	Unidirectional transmission
0x0000C0	FCTL_CSCMASK	Mask to get Cont Seq Condition
0x0000C0	FCTL_SEQDLY	Sequence to follow-delayed
0x000080	FCTL_SEQSOON	Sequence to follow-soon
0x000040	FCTL_SEQIMM	Sequence to follow-immediately
0x000000	FCTL_SEQNONE	No information
0x000030	FCTL_ASCMASK	Mask to get Abort Seq Condition
0x000030	FCTL_SEQABTR	Abort Seq - do ABTR
0x000020	FCTL_SEQSTOP	Stop seq

Table 42: Frame Control (F_CTL) Diagram (Continued)

Frame Control Field Bits (F_CTL)		
0x000010	FCTL_SEQABTS	Abort seq - do ABTS
0x000000	FCTL_SEQCONT	Continue seq
0x000030	FCTL_POLICYMASK	Mask to get seq policy
0x000030	FCTL_DISCRETX	Discard Multi Seq: Immed ReTx
0x000020	FCTL_PROCESS	Process policy with Infinite Buf
0x000010	FCTL_DISC1ABT	Discard single seq, abort
0x000000	FCTL_DISCMABT	Discard Multi seq, Abort
0x000008	FCTL_RELOFF	Relative Offset present
0x000004	FCTL_XCHREASS	Exchange Reassembly - reserved
0x000003	FCTL_FILLMASK	Mask to get the fill bits
0x060f00	FCTL_INVALID	class 1, compression, encryption
0xffff	NULL_XID	Unassigned ox_id or rx_id

Sequence ID (SEQ_ID)

Identifies and tracks all of the frames within a sequence between a source and destination port pair.

Sequence Count (SEQ_CNT)

Indicates the sequential order of frame transmission within a sequence, or multiple consecutive sequences, within the same exchange.

Originator ID (OX_ID)

Originator_ID (OX_ID) refers to the exchange ID assigned by the originator port.

Example

```
00:44:26.599  tFspf  Tx  8   40  02fffffd,00fffffd,0284ffff,14000000,10cac760
```

In the example above, `0284` is the Originator ID. See also Table 40 on page 368.

Responder ID (RX_ID)

The Responder_ID is assigned by the responder to the Exchange.

Example

```
00:44:26.599  tFspf  Tx  8   40  02fffffd,00fffffd,0284ffff,14000000,10cac760
```

In the above example, the `ffff` is the Responder ID. Refer also to Table 40 on page 368.

Data Field or Payload

The standard limits the minimum size to 2112 bytes. Refer to "The FC_PH Frame" on page 367 or Table 40 on page 368.

Type Code

The Type Code (Table 43) provides the type of protocol service (for example., FC_CT, FCP, FCIP and so on).

Table 43: Type Code

Type Code	
0x00	Basic Link
0x01	Extend Link
0x04	ISO/I?E?C? 8802-2 LLC
0x05	FCIP
0x08	SCSI_FCP
0x09	SCSI-GPP
0x20	Fibre Channel Services (NS,MS,AS,etc.)
0x21	FC-FG
0x22	FC_SW
0x23	FC-AL
0x24	FC-SNMP
0x25-0x27	Fabric Services
0x30-0x33	Scalable Coherent Interface
0x40	HIPPI-FP
0x58	Virtual Interface
0x5b	Fabric
0xe0-0xff	Vendor Specific

Data Field Control (DF_CTL)

This field indicates the presence of one or more optional headers at the beginning of the data field of the frame. Optional headers are used for information that may be required by some applications or protocol mappings. See Table 44.

Table 44: Data Field Control (DF_CTL) Optional Headers

DF_CTL	
0x40	SECURITY_HEADER
0x20	NETWORK_HEADER
0x10	ASSOCIATON_HEADER
0x03	DEVICE_HEADER
0x8c	DF_RESERVED

Class Specific Control Field (CS_CTL)

Different controls are necessary for different classes of service. This field is always zero per the standards. If it is non-zero, it is an HP internal code called *IU_Status Values* (see Table 45).

Table 45: Class Specific Control Field (CS_CTL) IU Status Values

HP Specified Internal Code: CS_CTL (IU Status Value)		
0x02	IU_P_RJT	Received P_RJT
0x03	IU_F_RJT	Received F_RJT
0x04	IU_P_BSY	Received P_BSY
0x05	IU_F_BSY	Received F_BSY
0x06	IU_F_BSY_LC	Received F_BSY_LC
0x10	IU_NO_EXCH	Cannot allocate exchange
0x11	IU_OFFLINE	Port is offline
0x12	IU_BAD_EXCH	Exchange ID not valid
0x013	IU_NO_ACK	ED_TOV expired
0x14	IU_CORRUPT	CRC err, encoding err, too long, and so on
0x15	IU_BAD_CLASS	Class 1 frame

Table 45: Class Specific Control Field (CS_CTL) IU Status Values (Continued)

HP Specified Internal Code: CS_CTL (IU Status Value)		
0x16	IU_BAD_S_ID	Invalid S_ID
0x17	IU_BAD_D_ID	Invalid D_ID, VC, or multicast address
0x18	IU_TIMED_OUT	Frame timed out, generate F_BSY
0x19	IU_TX_UNAVAIL	Tx unavailable, generate F_BSY
0x1a	IU_LOGIN_RQRD	Login required
0x1b	IU_PROTOCOL	Protocol error
0x1c	IU_RX_FLUSHED	Frame flushed by rx port
0x20	IU_ALPA_TMPNA	AL_PA temporarily not available
0x21	IU_ALPA_PMTNA	AL_PA permanently not available
0x22	IU_LOGO_OFFLINE	Logo received or port goes offline
0x23	IU_ZONE_CONFLT	Zone conflict
0x24	IU_ABTS_RX	Received an ABTS that flushed this IU
Async IU state, response		
0x80	IU_ASYNC_RESP	Async IU response payload received
0x81	IU_ASYNC_TO	Async IU response timeout
0x82	IU_ASYNC_ABTS	Async IU abtsed
0x83	IU_ASYNC_LOGO	Async IU killed due to port logout/offline
0x84	IU_ASYNC_ACKTO	Async IU ack timeout

State Change Notification (SCN)

There are three different State Change Notifications:

- "State Change Registration (SCR)" on page 376
- "Register State Change Notification (RSCN)" on page 376
- "Internal State Change Notification (SCN)" on page 376

SCN Definitions

State Change Registration (SCR)

The State Change Registration (SCR) Extended Link Service requests the Fabric Controller to add the N_Port or NL_Port to the list of N_Ports and NL_Ports registered to receive the Registered State Change Notification (RSCN) Extended Link Service.

Register State Change Notification (RSCN)

The Fabric Controller issues RSCN requests only to N_Ports and NL_Ports that have registered to be notified of state changes in other N_Ports and NL_Ports. This registration is performed via the State Change Registration (SCR) Extended Link Service. An N_Port or NL_Port may issue an RSCN to the Fabric Controller without having completed SCR with the Fabric Controller.

Internal State Change Notification (SCN)

The Internal State Change Notification is used for internal state change notifications, not external changes. This is the switch logging that the port is online or is an Fx_port. This is not what is sent from the switch to the Nx_ports. An SCN example is included on page 376.

Reading an SCN Event

The following examples show the same output from three different versions of firmware.

Example v3.x

```
portLogDump
time           task       event  port  cmd    args
---------------------------------------------------------------------------
12:05:28.116  tReceive   scn   13       0    137
```

See "SCN Codes and Descriptions" on page 377 to view the `cmd` description.

Example v4.0.x

```
time             task   event    port    cmd       args
----------------------------------------------------------------------
12:05:28.116    PORT    scn      13     137
```

See "SCN Codes and Descriptions" on page 377 to view the `cmd` description.

Example v4.2.x

```
time          task   event   port   cmd     args
----------------------------------------------------------------------
12:05:28.116   PORT   scn     7      137    00000000, 00000000, 00000008
```

- The `cmd` represents the SCN State. See "SCN Codes and Descriptions" on page 377 to view the `cmd` description.
- Read the argument columns as follows:
  - — Argument 1 is dependant on the SCN Type. For this example:
    - First 16-bits (Most Significant) = mode that the port is in. See "SCN Modes" on page 381.
    - Second 16-bits (Least Significant) = error that causes the port to be marked OFFLINE.
  - — Argument 2 is dependent on the SCN type; it is currently not used (00000000).
  - — Argument 3 is the SCN type. See "SCN Types" on page 381.
- Combine the SCN type (the third argument) and the SCN state (the **cmd** column) to uniquely identify a particular SCN. The SCN state alone is not sufficient, and is not guaranteed to be unique across all SCN types. See "SCN Types" on page 381 and "SCN States by Type" on page 379.

SCN Codes and Descriptions

The SCN codes described in Table 46 represent the SCN state, and appear in the **cmd** column of an SCN event. For v4.2.x, combine the SCN type (the third argument) and the SCN state (the **cmd** column) to uniquely identify a particular SCN. The SCN state alone is not sufficient, and is not guaranteed to be unique across all SCN types.

Table 46: Internal State Change Notification (SCN)

SCN Value	Status	Description
0	UNKNOWN	Port status is unknown.
1	ONLINE	Port is online (in active state).
2	OFFLINE	Port is offline.
3	TESTING	Port is in use by diagnostics.
4	FAULTY	Port is marked faulty.
5	E_PORT	Port is an E_Port.
6	F_PORT	Port is Fabric aware port (F or FL).
7	SEGMENTED	Port is segmented.
8	T_Port	Port is a trunking port, not trunk master.
9	AC_PORT	Port is active; link reset is done for E_Port or master trunk port.
10	LIP_ONLINE	Loop initialization occurred.
11	LR_Port	Port is active; link reset is done for non-E_Port.
12	FLOGI_DOC	FLOGI device.
13	FORCE_OFFLINE	Force OFFLINE a port that is already OFFLINE.
14	BUF_ONLINE	Became online by acquiring free buffers.
15	BUF_OFFLINE	Became offline due to lack of buffers.
16	Domain Valid	A valid domain was reported.
17	Domain Invalid	An invalid domain was reported.
18	Domain Reachable	A reachable domain was reported.
19	Domain Unreachable	An unreachable domain was reported.
20	Switch ONLINE	A switch came online.
21	Switch OFFLINE	A switch went offline.
22	Zoning Configuration Change	A zoning configuration change occurred.

Table 46: Internal State Change Notification (SCN) (Continued)

SCN Value	Status	Description
23	Watchdog probe timer expired	The Watchdog software (which monitors Fabric OS modules on the kernel) probing timer expired.
24	Software Watchdog register request	The Watchdog software (which monitors Fabric OS modules on the kernel) sent a register request.
128	FCP message probe, start probing	Fibre Channel Protocol - message probing started.
129	FCP message flush, stop probing	Fibre Channel Protocol - message probing stopped.
135	NS message update area	Name Server update area.
136	NS message add area	Name Server add area.
137	NS message delete area	Name Server message delete area.
138	Route all done	Both domain and are routes are done.
144	ROUTE_ALL_DONE	Both domain and are routes are done.

SCN States by Type

Table 47 specifies SCN states.

Table 47: SCN States Displayed By Type

Code	Status	Description
PORT_SCN Type		
0	UNKNOWN	Port status is unknown.
1	ONLINE	Port is online (in active state).
2	OFFLINE	Port is offline.
3	TESTING	Port is in use by diagnostics.
4	FAULTY	Port is marked faulty.
5	E_PORT	Port is an E_Port.
6	F_PORT	Port is an F_port.
7	SEGMENTED	Port is segmented.
8	T_PORT	Port is a trunking port, not trunk master.

Table 47: SCN States Displayed By Type (Continued)

Code	Status	Description
10	LIP_ONLINE	Loop initialization occurred.
121	FORCE_OFFLINE	Force OFFLINE a port that is already OFFLINE.
122	BUF_ONLINE	became online by acquiring free buffers.
123	BUF_OFFLINE	became offline due to lack of buffers.
SWITCH_SCN Type		
16	DOMAIN_VALID	
17	DOMAIN_INVALID	
18	DOMAIN_REACHABLE	
19	DOMAIN_UNREACHABLE	
20	SW_ONLINE	
21	SW_OFFLINE	
22	CFG_CHANGED	
23	SWD_SWITCH_HEARTBEAT_REQ	
24	SWD_SWITCH_REGISTER_REQ	
25	PASSWD_CHANGED	
FAB_SCN Type		
9	AC_PORT	Port is active; link reset is done for E_Port or master trunk port.
11	LR_PORT	Port is active; link reset is done for non-E_Port.
26	SW_PERSISTENT_DISABLE	Sent when the switch is ready, that is, after POST if POST is running, and the switch is currently persistently disabled.
SEC_SCN Type		
27	REM_DOMAIN_SET	Routes to remote domain are set up.
28	REM_DOMAIN_CLEAR	Routes to remote domain are cleared.
120	FLOGI_DCC	FLOGI device.
FCP_SCN Type		
128	FCPMSG_PROBE	
129	FCPMSG_FLUSH	
UPD_SCN Type		

Table 47: SCN States Displayed By Type (Continued)

Code	Status	Description
135	NSMSG_UPD_AREA	
136	NSMSG_ADD_AREA	
137	NSMSG_DEL_AREA	
144	ROUTE_ALL_DONE	
GBIC_SCN Type		
1	ONLINE	Module in.
2	OFFLINE	Module out.

SCN Types

The SCN types in Table 48 appear in Argument 3. See “Example v4.2.x” on page 377.

Table 48: Types of SCNs

Code	Abbreviation	Description
0x00000001	SWITCH_SCN	Switch state change notification
0x00000002	PORT_SCN	Port state change notification
0x00000008	UPD_SCN	Update state change notification
0x00000100	ZONE_SCN	Zone check
0x00000400	FCP_SCN	FCP
0x00000800	GBIC_SCN	GBIC (SFP) module in/out scn
0x00010000	FAB_SCN	Fabric application
0x00040000	SEC_SCN	FLOGI device violation

SCN Modes

SCN Modes in Table 49 appear in the first bit of Argument 1 for a port_scn type. See “Example v4.2.x” on page 377.

Table 49: SCN Modes

Value	SCN Modes
0	PORT_SCN_MODE_NORMAL
1	PORT_SCN_MODE_DISABLED
2	PORT_SCN_MODE_LOOPBACK
3	PORT_SCN_MODE_BYPASSED

SCN Errors

The SCN errors in Table 50 appear in the second bit of Argument 1 in a port_scn type output. See “Example v4.2.x” on page 377.

Table 50: SCN Errors

Value	Name
0	PORT_SCN_ERR_NO_ADDITIONAL_INFO
1	PORT_SCN_ERR_NO_MODULE
2	PORT_SCN_ERR_NO_LIGHT
3	PORT_SCN_ERR_NO_SYNC
4	PORT_SCN_ERR_NOT_ONLINE
5	PORT_SCN_ERR_FAULT
6	PORT_SCN_ERR_LASER_FAULT

Specific Codes

ASIC Loop Codes

Table 51 specifies the ASIC loop codes.

Table 51: Specific ASIC Loop Codes

cmd	Loop SCN Reason Code	Description
LIP	0x0	Loop entering OPEN_INIT state.
	0xA45	
	0x5F4A	
	0x8001	Retry loop init.
	0x8002	Start loop after gaining sync.
	0x8003	Restart loop after port reset.
	0x8004	Lip the loop after loop timeout.
	0x8005	Retransmitting LIP in ARBF0.
	0x8006	Lip the loop if OPN(x,y) returns.
	0x8007	Start loop when transit out of G_Port.
	0x8008	Start loop if self loopback.
	0x8009	Per N_Port FLA LINIT ELS.
	0x800a	Per N_Port FLA LPC ELS.
	0x800b	Per QL LOOP_LIP.
	0x800c	Per QL LOOP_INIT.
	0x800d	LIP due to loop rdx buffer overflow.
	0x800e	Start loop because of loop diagnostic.
	0x800f	Per new Phantoms being added.
	0x8010	Per new Phantom being added (IPO).
	0x8011	`bloominitretry` - loop init timed out.
	0x8012	`bloominitretry` - stuck at init state.
	0x8013	`bloominitretry` - no RSVD mini-buf for LISM.
	0x8014	`bloominitretry` - not pt-to-tp capable.
	0x8015	`bloomInitRetry` - no LISM rx in 2 AL_TIME.
	0x816	`bloomStopLinit` - L to F transition.
	F7F7	The loop port in the initializing state is requesting loop initialization but does not currently have a valid AL_PA.

Table 51: Specific ASIC Loop Codes (Continued)

cmd	Loop SCN Reason Code	Description
	(F7,AL_PS)	The loop port identified by the AL_PS value is requesting loop initialization.
	(F8,AL_PS)	A loop interconnection has failed.
	(AL_PD,AL_PS)	The Selective Reset LIP is used to perform a vendor specific reset at the loop port specified by the AL_PD value. AL_PD=FF is a destination indicating all ports.
TMO	D6	LIP time out. The looplet loop initialization timed out.
BMP	D3	Looplet AL_PA bitmap. Loop Init completed, FL_Port in monitoring state.
LIM	D2	LISM completed, FL_Port became the loop master.
OLD	D5	Port transited to the old_port state.
OLP	D0	Offline.

Port Physical State Values

Table 52 specifies physical state values.

Table 52: Specific Physical State Values

State	Description
NO_CARD	No optional card installed (Check license key).
NO_Module	No GBIC module installed.
LASER_FLT	Laser fault.
NO_LIGHT	No light being received.
NO_SYNC	Out of Synchronization.
IN_SYUNC	In Synchronization.
PORT_FLT	Port Fault.
DIAG_FLT	Diagnostic Fault.
LOCK_REF	Receiver Locking Reference Clock.
Unknown	Port status is unknown.

LED State Values

Table 53 specifies LED state values.

Table 53: Specific LED State Values

LED State	Description
STEADY_BLACK	No light
STEADY_YELLOW	Receiving light, but not yet online
SLOW_YELLOW	Disabled (diagnostics or portDisable)
FAST_YELLOW	Error, fault with port
STEADY_GREEN	Online and ready to go
SLOW_GREEN	Online but segmented
FAST_GREEN	Online in internal loopback
FLICKERING	Online and traffic flowing through port
YELLOW_GREEN	Bypass

Bypass Reason Codes

Table 54 specifies bypass reason codes.

Table 54: Specific Bypass Reason Code

Code	Reason
1	Disabled
2	Potential E_Port
3	QL task issued bypass

Switch Parameter Meanings

Table 55 specifies switch parameter meanings.

Table 55: Specific Switch Parameter Meanings

Parameter	Meaning
TACHYON	Better IP behavior with Tachyon
ISOLATED	Do not probe for E_Ports
NOTYPES	Do not probe for broadcast or multicast
VCINDID	VC encoding in DID

Table 55: Specific Switch Parameter Meanings (Continued)

Parameter	Meaning
USECSCTL	Use CS_CTL in FC_header for vc
NOCLASSF	Turn class 2 frames into class F frames
DISTANCE	Long distance fabric
PID256FORMAT	Use 256-port pid format
VCXLTLINIT	Link init protocol for setup vcxlt mode; note this is port wide config sent through op_mode in ELP

Speed Negotiation

Speed Negotiation Code Commands

Table 56 describes the speed negotiation code commands.

Table 56: Speed Negotiation Code Commands

Abbreviation	Code	Description
NC	01	Negotiation complete with speed 1G.
NC	02	Negotiation complete with speed 2G.
NF		Negotiate follow.
NM		Negotiate master.
WS	00	Signal is okay and actual start of SN - “trigger for start”.
	01	Signal is okay and actual start of SN - “trigger for start”.
	aa	Speed negotiation started in attach( ) - “stay armed”.

Speed Negotiation EVENT

Table 57 describes the speed negotiation event.

Table 57: Speed Negotiation Event

Output	Description
0xaa	SN_ATTACH
0xb0	SN_LASER_FAIL
0xc0	SN_RX_IBM_SIG_LOSS
Oxd0	SN_WD_TIMEOUT
0xe0	SN_RX_SIG_LOSS
0xee	SN_RX_SIG
0xf0	SN_RX_SYNC_LOSS
0xff	SN_RX_SYNC
0x01	SN_INCONSISTENT

Speed Negotiation State Values

Table 58 describes the speed negotiation state values.

Table 58: Speed Negotiation State Values

Code	Abbreviation	Description
0	SPEED_NEGO_INIT	Entry to state machine.
18	WAIT_FOR_SIGNAL_18	Wait for signal state corr to box 18.
11	WAIT_FOR_SIGNAL_11	State .. box 11.
20	NEGOTIATE_MASTER_20	Neg master state corr to box 20.
21	NEGOTIATE_MASTER_21	State .. box 21.
27	NEGOTIATE_MASTER_27	State .. box 27.
31	NEGOTIATE_FOLLOW_31	Neg follow state corr to box 31.
34	NEGOTIATE_FOLLOW_34	State .. box 34.
40	NEGOTIATE_COMPLETE	Speed negotiation complete.
50	SN_INSYNC	SN done; for RX_FIFO int do not start sn.

DISTANCE Code Value

Table 59 specifies distance code values.

Table 59: Code Value for Distance

Distance	Value
NORMAL_DISTANCE	No special long distance consideration
VERY_LONG	Level one long distance < = 50km
SUPER_LONG	Level two long distance < = 100km

I/O Control (ioctl)

An IOCTL event is an internal message that gives information about the port and the stage of bring-up or take-down of the ports. See “Speed Negotiation Example” on page 398 for information on reading an IOCTL event.

IOCTL CTL Codes

Table 60 specifies IOCTL CTL codes.

Table 60: IOCTL CTL Codes

Ioctl Code	Description and Interpretation Argument
0x00	Enable chip level port interrupt
0x01	Entry describes physical port
0x02	Entry describe WWN
0x04	Entry describes Al-PA bitmap
0x20	Enable free buffer interrupt
0x30	Get buffer and buffer port
0x31	Set available buffer interrupt
0x32	Return buffer
0x33	Get Fx port error status
0x34	Get Fl port error status
0x35	Get physical state
0x36	Set physical state
0x37	Set FCTL_mode

Table 60: IOCTL CTL Codes (Continued)

Ioctl Code	Description and Interpretation Argument
0x38	Get device information
0x39	Get loop bmp
0x3a	Set E_Port flow control mode
0x3b	Get register map
0x3c	Return Tx buffer
0x3d	Filter processing stages
0x3e	Filter processing stage 2
0x3f	Software frame filtering
0x40	Remove all phantom nodes for port
0x41	Add a phantom device (loop only)
0x42	Translate phantom sid and did
0x43	Create phantom node for remote did
0x44	Get blm_my_alpa table from ASIC
0x45	Get blm_plt_cam table from ASIC
0x46	Get blm_plt_alpa table from ASIC
0x50	Test phantom for (S_ID, D_ID)
0x51	Add a phantom device (loop only)
0x52	Remove a phantom device
0x53	Get phantom AL_PA by address ID
0x54	Get address ID by phantom AL_PA
0x55	Looplet init (send LIPs)
0x56	Looplet init sequence Argument: 1,0
0x57	Loop port (or looplet) bypass
0x58	Looplet init AL_PA bitmaps. Bitmap, IU pointer
0x59	Looplet Unicast Routes
0x5a	Set up port for loop diag mode
0x5b	Loop port bypass the ALPD
0x5c	Loop port enable the ALPD

Table 60: IOCTL CTL Codes (Continued)

Ioctl Code	Description and Interpretation Argument
0x60	Write/read 64-bytes to/from the RAM buffer
0x61	Get cmem status
0x62	Check if FL_Port a loopback sla
0x63	Set buffer line value and offset. 1,1
0x64	Disable FC-AL transmit front-end
0x65	Enable FC-AL transmit front-end
0x66	Set FL_Port to be cable loopback. Interpretation Argument: Port#, 0
0x67	Clear Diag mode flag
0x70	FLA Loop INITializing
0x71	FLA Loop Port Control
0x72	FLA Loop Status
0x73	LPORT ALPA bitmap
0x80	Port administration data. The ports are set up while the switch is booting up "a,0"
0x81	Get common hardware statistics
0x82	Get loop hardware statistics
0x83	Get hardware frame statistics
0x84	Get hardware error statistics
0x85	Get interrupt statistics
0x86	Get available BB_Credit
0x87	Get bb credit for the Fx_PORT
0x88	Get public/private/phantom counts
0x8e	Get GBIC module type
0x8f	Port performance calculation
0x90	Get credits for all E_Port VCs. Credit values, 0 (0 = done)
0x91	Set credits for all E_Port VCs. Credit values, 0 (0 =done)

Table 60: IOCTL CTL Codes (Continued)

Ioctl Code	Description and Interpretation Argument
0x92	Get BB-Credit for the Fx_Port. IU pointer, 0 (0 = done)
0x93	Set up port for loop diag mode
0x94	Loop port bypass the ALPD
0x95	Loop port enable the ALPD
0x96	Get port topology
0x97	Set port topology
0x99	LIP the loop, TX_UNAVAIL on/off
0x9a	Send MRK primitive signal
0xa0	LED control
0xa1	Port is an E_Port. Interpretation Argument: 0,0
0xa2	Port is an F_Port. Native address, value
0xa3	Port is segmented Interpretation Argument: 0,0 (done)
0xa4	Domain name is known Domain#, 0 (Note - 0 means “done”)
0xa5	Bring port online
0xa6	Take port offline
0xa7	Take port into Link Reset
0xa8	Add unicast route. Port#, cmd (cmd 1 = building)
0xa9	Delete unicast route Argument = Port#, port#
0xaa	Add multicast route Argument = Well Known Address, port#
0xab	Delete multicast route Argument = Well Known Address, port#

Table 60: IOCTL CTL Codes (Continued)

Ioctl Code	Description and Interpretation Argument
0xac	Unicast routing table done Argument = 0,0 (0,0 = done)
0xad	Multicast routing table done Argument: 0,0 (0,0 = done)
0xae	Undo a previous F_Port ioctl
0xaf	Take a port down then up Argument = 0,0 (0,0 = done)
0xb0	Enable hardware zoning Argument = 0,0 (0,0 = done)
0xb1	Disable hardware zoning Argument = 0,0 (0,0 = done)
0xb2	Add members to zone
0xb3	Delete member from zone
0xb4	Add a zone type
0xb5	Add zone group
0xb6	Enable all port zoning
0xb7	Reset all port zoning
0xb8	Disable all port zoning
0xb9	Free zoning token
0xba	Set up FLOGI command tgrap
0xbb	Set up report lun cmd trap
0xbc	Get World Wide Name and IDs
0xbd	Get receiver/originator ID
0xbe	Add LUN information
0xbf	Exclude port from zoning
0xc0	Get port interrupt bit map
0xc1	Enable port interrupt
0xc2	Disable port interrupt
0xc3	Check if port intr pending

Table 60: IOCTL CTL Codes (Continued)

Ioctl Code	Description and Interpretation Argument
0xc4	Enable chip interrupt, SW12K
0xd0	Add a SID_DID pair
0xd1	Delete a SID_DID pair
0xd2	Get the list of EE keys
0xd3	Get the current EE mask
0xd4	Set the SID-ID pair
0xd5	Clear the CRC counter for ALPA
0xd6	Get the CRC counter for ALPA
0xd7	Send word count for SID_DID pair
0xd8	RCV word count for SID_DID pair
0xd9	CRC err count for SID_DID pair
0xdc	Auto speed negative mode for argument1 value
0xdd	Get port speed ala admin.h defines Argument: value, 0
0xde	Port speed capability ala admin.h Argument: Port speed value, 0
0xdf	Get the port's long distance level Argument: Value, 0
0x13d	Argument: IU address pointer
0x13e	Argument: IU address pointer, 0
0xe0	Send MARK primitive onto wire Argument: 0,0
0xe1	Get the MARK timestamps Argument: 0,0
0xe2	Add the port to the trunk Argument: 0,0
0xe3	Get all trunk masters on the quad Argument: IU address pointer, IU address pointer
0xe4	Update MARK timestamp with RMT

Table 60: IOCTL CTL Codes (Continued)

Ioctl Code	Description and Interpretation Argument
0xe5	Check whether port is trunkable Argument = Port #, IU address pointer
0xe6	Enable trunking if possible Argument = IU address pointer, IU address pointer
0xe7	Get trunking group information
0xe8	Get ISL band width Argument = IU address pointer, 0
0xf0	Add a filter counter
0xf1	Delete a filter counter
0xf2	Number of filter hit count
0xf3	Add get perf filter references
0xf4	Clear filter hit counts
0xf5	Clear all filter counts for port
0x100	Get fail detection logic statuses Argument = IU address pointer, 0
0x101	Set fail detection control bit
0x102	Clear fail detection control bit
0x103	Set Rx_to_Tx parity control
0x104	Get Rx-to-Tx parity error status
0x105	Get Rx-to-Tx parity error status
0x106	Enable fail detection interrupt
0x107	Disable fail detection interrupt
0x108	Check for fail detection interrupt
0x120	Enable IPO zoning
0x121	Disable IPO zoning
0x122	Fabric lookup report after enable
0x123	Name server list of PIDs for IPO
0x124	Query if node is IPO target/host

Table 60: IOCTL CTL Codes (Continued)

Ioctl Code	Description and Interpretation Argument
0x125	Ask for list of nodes to zone check
0x126	List of IPO hosts zoned to target
0x127	RSCN received
0x128	List of IPO targets zoned to host Argument = IU address pointer, 0
0x129	Check for existence of IPO hosts
0x12a	Fabric merge report after reconfigure
0x12b	Switch online SCN received
0x12c	add unicast single area route Argument = 0,0
0x130	Add zone type (new) Argument = IU address pointer, IU address pointer
0x131	Add zone group (new) Argument = IU address pointer, IU address pointer
0x132	Enable all port zoning (new) Argument = : 0,0
0x133	Reset all port zoning (new) Argument = 0,0
0x134	Disable all port zoning (new) Argument = 0,0
0x135	Free zoning token (new) Argument = IU address pointer, 1
0x136	Set up PLOGI command trap (new) Argument = 0,0
0x137	Set up report lun cmd trap (new)
0x138	Get World Wide Name and IDs (new) Argument = IU address pointer, IU address pointer
0x139	Get receiver/originator ID (new)

Table 60: IOCTL CTL Codes (Continued)

Ioctl Code	Description and Interpretation Argument
0x13a	Apply LUN information (new)
0x13b	Exclude port from zoning (new)
0x13c	Soft zoning port (new)
0x13d	Get frame filtering features (new)
0x13e	Set frame filtering features (new)
0x13f	Clear port zoning except dyn flt
0x140	Load sidcam (diagnostic)
0x141	Load didcam (diagnostic)
0x142	Load LUN offset registers (diagnostic)
0x143	Load zone group RAM (diagnostic)
0x144	Load zone horizontally (diagnostic)
0x145	Load filter selection (diagnostic)
0x146	Load field definition (diagnostic)
0x147	Load action registers (diagnostic)
0x148	Get filter statistics (diagnostic)
0x149	Clear all filtering hardware (diagnostic)
0x14a	Enable frame filtering (diagnostic)
0x14b	Disable frame filtering (diagnostic)
0x150	Zone rscn handling Argument: IU address pointer, 0
0x151	Remove related CAM entries on all ports
0x160	Set alpa in blm_alpa_avail[ ] reg
0x161	Clear alpa in blm_alpa_avail[ ] reg
0x170	Freeze RT used by diags: EMC ESSLB
0x180	Get chip Time of Day
0x181	Get chip Time of Day Prescaler
0x182	Set chip Time of Day Prescaler
0x183	Get RX TOD Pre-Confirmed

Table 60: IOCTL CTL Codes (Continued)

Ioctl Code	Description and Interpretation Argument
0x184	Set RX TOD Pre-Confirmed
0x185	Get RX TOD Active
0x186	Set RX TOD Active
0x187	Set RX TOD Prescaler
0x188	Set RX TOC
0x189	mS to TOD click conversion
0x190	TOD click to mS conversion
0x191	Get VC translation link init
0x192	Send MARK primitive with LRTT (link round trip timer) enabled
0x193	Enable MARK retransmission
0x194	Disable MARK retransmission
0x195	Save link round trip timer from ASIC to BLOOM driver structure
0x196	Set link round trip delay in ASIC driver structure
0x197	Called from Panic to disable all ports' RX
0x198	Get vcc credit of online E-port

Speed Negotiation Example

```
20:07:07.896  interrupt   sn        3   WS  00f0,00000015,00000002
20:07:07.929  tFabric     ioctl     3  150  10272720,0
20:07:08.146  interrupt   scn       3    2        0x00000003
20:07:08.179  tFspf       ioctl     3   dd  10260e40,0
20:07:08.179  tFspf       ioctl     3   a9  1,e
20:07:08.179  tFspf       ioctl     3   a9  2,e
20:07:08.179  tFspf       ioctl     3   a9  3,e
20:07:08.179  tFspf       ioctl     3   a9  4,e
20:07:08.179  tFspf       ioctl     3   a9  5,7
20:07:08.179  tFspf       ioctl     3   a9  6d,e
20:07:08.179  tFspf       ioctl     3   a9  71,7
20:07:08.179  tFspf       ioctl     3   a9  72,e
20:07:08.179  tFspf       ioctl     3   a9  74,e
20:07:08.179  tFspf       ioctl     3   a9  75,e
20:07:08.179  tFspf       ioctl     3   a9  76,e
20:07:08.179  tFspf       ioctl     3   a9  ef,e
20:07:08.179  tFspf       ioctl     3   ab  fffb00,e      * 255
20:07:08.529  tReceive    sn        3   NC  0001,00000000,00000004
20:07:08.529  tReceive    loopscn   3  LIP  8002

============
20:14:38.385  SPEE        sn       30   WS  00000000,00000000,00000000
20:14:38.389  SPEE        sn       30   WS  000000ee,00000000,00000000
20:14:38.395  SPEE        sn       30   WS  00000001,00000000,00000000
20:14:38.995  SPEE        sn       30   NC  00000001,00000000,00000001
20:14:38.996  LOOP        loopscn  30  LIP  8002
20:14:39.021  LOOP        loopscn  30  LIP  f7f7
20:14:39.022  PORT        Tx3      30   12  22000000,00000000,ffffffff,11010000
20:14:39.058  PORT        Rx3      30   12  22000000,00000000,ffffffff,11010000
20:14:39.060  LOOP        loopscn  30  LIM  0
```

Extended Link Service (ELS)

About FC_PH ELS

Extended Link Services (ELS) are sent to the destination N_port to perform the requested function or service.

- The R_CTL field of an Extended Link Service request is always set to 0x22.
- The R_CTL field of the Extended Link Service reply is set to 0x23.
- The type filed for both requests and replies is 0x01 (`portlogdump` trace does not provide the TYPE information).

The command code for an ELS is always the first word of the payload (word 6) for both the request and reply.

There are 2148 bytes in a frame; the `portlogdump` captures a portion of the frame.

For Tx and Rx events, the first Argument field obtains the portion of the header and one word of the payload, word6. Arguments 1, 2 and 3 belong to the FC_PH header (word 0,1,4 = R_CTL,D_ID,S_ID,OX_ID,RX_ID). The last argument (4th argument) belongs to the payload. See “ELS Examples” on page 406.

ELS Command Codes

Table 61 specifies the ELS command codes.

Table 61: ELS Command Codes

ELS Command	Abbreviation	Description
01000000	RJT	Reject
02000000	ACC	Accept
03000000	PLOGI	N_Port Login
04000000	FLOGI	F_Port Login
05000000	LOGO	Logout
06000000	ABTX	Abort Exchange
07000000	RCS	Read Connection Status
08000000	RES	Read Exchange Status Block
09000000	RSS	Read Sequence Status Block

Table 61: ELS Command Codes (Continued)

ELS Command	Abbreviation	Description
0A000000	RSI	Request Sequence Initiative
0B000000	ESTS	Establish Streaming
0C000000	ESTC	Estimate Credit
0D000000	ADVC	Advise Credit
0E000000	RTV	Read Timeout Value
0F000000	RLS	Read Link Status
10000000	ECHO	ECHO
11000000	TEST	Test
12000000	RRQ	Reinstate Recovery Qualifier
20100000	PRLI	Process Login
21100000	PRLO	Process Logout
22000000	SCN	State Change Notification
23000000	TPLS	Test Process Login State
24000000	TPRLO	Third Party Process Logout
25000000-2F000000	Unused	
30000000	GAID	Get Alias ID
31000000	FACT	Fabric Activate Alias ID
32000000	FDACT	Fabric Deactivate Alias ID
33000000	NACT	N_Port Activate Alias ID
34000000	NDACT	N_Port Deactivate Alias ID
35000000-3F000000	Unused	
40000000	QoSR	Quality of Service Request
41000000	RVCS	Read Virtual Circuit Status
42000000-4F000000	Unused	
50000000	PDISC	Discover N_Port Service Parameters
51000000	FDISC	Discover F_Port Service Parameters

Table 61: ELS Command Codes (Continued)

ELS Command	Abbreviation	Description
52000000	ADISC	Discover Address
53000000	RNC	Report Node Capability
54000000	FARP	FC Address Resolution Protocol
55000000-5F000000	Unused	
60000000	FAN	Fabric Address Notification
61000000	RSCN	Registered State Change Notification
62000000	SCR	State Change Registration
63000000-6F000000	Unused	
70000000	LINIT	Loop Initialize
71000000	LPC	Loop Port Control
72000000	LSTS	Loop Status
73000000-77000000	Unused	
78000000	RNID	Request Node Identification Data
79000000	RLIR	Registered Link Incident Record
7A000000	LIRR	Link Incident Record Registration
7B000000-FF000000	Unused	
11010000	LISM	Select Master
11020000	LIFA	Fabric Assigned
11030000	LIPA	Previously Acquired
11040000	LIHA	Hard Assigned
11050000	LISA0	Soft Assigned (old)
11050100	LISA1	Soft Assigned (new)
11060000	LIRP	Report Position
11070000	LILP	Loop Position

FC-PH - Reject Reason Codes and Explanations

See “Switch Fabric Internal Link Services (SW_ILS)” on page 409 for a complete list.

FC-PH Reject Reason Codes

Table 62 specifies FC-PH reject reason codes.

Table 62: FC-PH Reject Reason Codes

Reason Code	Description
01	Invalid ELS Command Code – the command code is not recognized by the recipient.
02	Invalid revision level. The recipient does not support the specified revision level.
03	Logical Error – The request identified by the command code and the payload content is invalid or logically inconsistent for the conditions present.
04	Invalid payload size – The size of the payload is inconsistent with the command code and/or any length fields in the payload.
05	Logical Busy – the port is unable to perform the request at this time. Busy reason explanation code: 01 – PHYSICAL_N_PORT_BUSY 03 – N_PORT_RESOURCE_BUSY
07	Protocol Error – an error has been detected that violates FC-2 protocols and is not covered by another reason code.
09	Unable to perform command request – the recipient is unable to perform the request at this time.
0B	Command not supported – the recipient does not support the ELS command.
Others	Reserved.
FF	Vendor-unique field indicating an error condition.

FC-PH Reject Explanation

F_JRT information relates to the F_Port. P_RJT information relates to the N_Port.

Table 63 provides explanation codes for FC-PH reject reasons.

Table 63: FC-PH Reject Reason Explanation Codes

Code	Description	Explanation
0x00	NO_ADDITIONAL_EXPLANATION	N/A
0x01	INVALID_D_ID	F_RJT - the Fabric is unable to locate the destination N_Port address. P_RJT - the N_Port which received this frame does not recognize the D_ID as its own Identifier.
0x02	INVALID_S_ID	F_RJT - the S_ID does not match the N_Port Identifier assigned by the Fabric. P_RJT - the destination N_Port does not recognize the S_ID as valid.
0x03	NOT_AVAIL_TEMP	F_RJT - The N_Port specified by the D_DID is a valid destination address, but the N_Port is not functionally available. For example, the N_Port is online and may be performing a Link Recovery Protocol.
0x04	NOT_AVAIL_PERM	F_RJT - The N_Port specified by the D_ID is a valid destination address, but the N_Port is not functionally available. The N_Port is offline, or powered down.
0x05	CLASS_NOT_SUPPORTED	F_RJT or P_RJT - The Class of Service (COS) specified by the Start of Frame (SOF) delimiter of the frame being rejected is not supported.
0x06	DELIMITER_ERROR	Deliminator usage error. F_RJT or P_RJT - The Start of Frame (SOF) or End of Frame (EOF) is not appropriate for the current conditions. For example, a frame started by SOFc1 is received while a Class 1 Dedicated Connection already exists with the same N_Port.
0x07	TYPE_NOT_SUPPORTED	F_RJT or P_RJT - The TYPE field of the frame being rejected is not supported by the port replying with the Reject frame.

Table 63: FC-PH Reject Reason Explanation Codes (Continued)

Code	Description	Explanation
0x08	INVALID_LINK_CONTROL	P_RJT - The command specified in the Information Category bits within R_CTL field in the frame being rejected is invalid or not supported as a Link_Control frame.
0x09	INVALID_R_CTL	P_RJT - The R_CTL field is invalid or inconsistent with the other Frame Header fields or conditions present.
0x0a	INVALID_F_CTL	P_RJT - The F_CTL field is invalid or inconsistent with the other Frame_Header field or conditions present.
0x0b	INVALID_OX_ID	P_RJT - The OX_ID specified is invalid, or inconsistent with the other Frame_Header field or conditions present.
0x0c	INVALID_RX_ID	P_RJT - The RX_ID specified is invalid, or inconsistent with the other Frame_Header field or conditions present.
0x0d	INVALID_SEQ_ID	P_RJT - The SEQ_ID specified is invalid, or inconsistent with the other Frame_Header field or conditions present.
0x0e	INVALID_DF_CTL	P_RJT - The DF_CTL field is invalid.
0x0f	INVALID_SEQ_CNT	P_RJT - The SEQ_CNT specified is invalid, or inconsistent with the other Frame_Header field or conditions present. A SEQ_CNT reject is not used to indicate out of order or missing data frames.
0x10	INVALID_PARAMETER	P_RJT - The Parameter field is incorrectly specified, or invalid.
0x11	EXCHANGE_ERROR	P_RJT - An error has been detected in the Identified Exchange (OX_ID). This could indicate data frame transmission without sequence initiative or other logical errors in handling an exchange.

Table 63: FC-PH Reject Reason Explanation Codes (Continued)

Code	Description	Explanation
0x12	PROTOCOL_ERROR	P_RJT - This reject code indicates that an error has been detected that violates the rules of FC-2 signaling protocol, which are not specified by other error codes.
0x13	INCORRECT_LENGTH	F_RJT or P_RJT - The frame being rejected is an incorrect length for the conditions present.
0x14	Unexpected_ACK	P_RJT - An ACK was received from an unexpected S_ID. The ACK received was not for an open sequence or exchange, but was received from a logged-in N_Port.
0x15	Reserved	
0x16	Login_Required	F_RJT or P_RJT - An exchange is being initiated before the interchange of service parameters (login, for example) has been performed. F_RJT may be issued by the fabric in order to notify an N_Port that a login with the fabric is required due to changes within the fabric. F_RJT is not issued by the fabric in order to convey login status of a destination N_Port.
0x17	Excessive_Sequences_Attempted	P_RJT - A new sequence was initiated by an N_Port which exceeded the capability of the sequence recipient as specified in the service parameters during login.
0x18	Unable_to Establish_Exchange	P_RJT - A new exchange was initiated by an N_Port, which exceeded the capability of the responder facilities.
0x19	Expiration_Security_Header not supported.	P_RJT - The N_Port does not support the optional Expiration_Security_Header.

Table 63: FC-PH Reject Reason Explanation Codes (Continued)

Code	Description	Explanation
0x1a	Fabric_Path_Not_Avail	F_RJT - The speed of the source and destination N_Ports does not match. Other fabric characteristics related to multiple fabric domains may also use this reason code.
0x1b	Vendor Unique Error	F_RJT or P_RJT - The Vendor Unique Reject bits (bits 7 - 0) are used by specific vendors to specify additional reason codes.
0x1c	Reserved	N/A

ELS Examples

For a text description of the events displayed in this example, see page 407.

ELS Example 1

v3.x Output

```
    time          task      event port cmd args
-------------------------------------------------
1. 22:55:51.199  tFcp      Tx3    12    16   220a1cef,00fffc0a,013effff,05000000,10d0d930
2. 22:55:51.199  tReceive Rx3    12     4   23fffc0a,000a1cef,013effff,02000000,10ca5ae0
```

Line 1.

```
22:55:51.199  tFcp  Tx3  12   16  220a1cef,00fffc0a,013effff,05000000,10d0d930
```

Table 64 explains the line 1 ELS arguments.

Table 64: ELS Argument Explanation Line 1

Argument 1	Argument 2	Argument 3	Argument 4	Argument 5
22 Routing Control Bits (R_CTL), page 368	00 = Identifier	013e "Originator ID (OX_ID)" on page 372	05000000 (log out) "ELS Command Codes" on page 399	10d0d930 IU address pointer (not available in v4.x). See "About the IU Pointer" on page 366.
0a1cef "Destination_ID (D_ID)" on page 370	fffc0a "Source_ID (S_ID)" on page 370	ffff "Responder ID (RX_ID)" on page 372		

Line 2

```
22:55:51.199  tReceive   Rx3  12  4  23fffc0a,000a1cef,013effff,02000000,10ca5ae0
```

Table 65 explains the line 2 ELS arguments.

Table 65: ELS Argument Explanation Line 2

Argument 1	Argument 2	Argument 3	Argument 4	Argument 5
23 (response) "Routing Control Bits (R_CTL)" on page 368	00 = Identifier	013e "Originator ID (OX_ID)" on page 372	05000000 (log out) "ELS Command Codes" on page 399	10d0d930 IU address pointer (not available in v4.x). See "About the IU Pointer" on page 366.
fffc0a "Destination_ID (D_ID)" on page 370	a1cef "Source_ID (S_ID)" on page 370	ffff "Responder ID (RX_ID)" on page 372		

Example Summary

In Example 2, the embedded port `ffffc0a` does an Extended Link Service (ELS) request logout from device `0a1cef`. Device `0a1cef` accepts the request.

ELS Example 2

```
12:32:53.583 tReceive Rx3 0 116 22fffffe,00000000,000cffff,04000000
```

where:

`0x22` = R_CTL - Extended Link Services Request
`0xfffffe` = Fabric F_port
`0x000000` = S_ID (attaching device does not yet have a fabric address.

Example Summary

Example 2 is an FLOGI frame to the fabric F_port (R_CTL=0x22, Extended Link Services Request; D_ID=`0xfffffe`, fabric F_port; S_ID=`0x000000`). The S_ID = 0 indicates that the attaching device does not yet have a Fabric address.

ELS Example 3

```
12:23:12.049 tReceive scn   1  6
12:23:12.049 tFspf    ioctl 1  dd  10129da0,0* 2
12:23:12.049 tFspf    ioctl 1  ac  0,0
12:23:12.049 tFspf    ioctl 1  aa  ffffff,10
12:23:12.049 tFspf    ioctl 16 aa  ffffff,1
12:23:12.049 tFspf    ioctl 1  ad  0,0
12:23:12.049 tFspf    ioctl 1  92  101f466c,0
12:23:12.049 tFspf    Tx3   1  116 23d31100,00fffffe,02220185,02000000
```

where:

`0x23` = Extended Link Services Reply (R_CTL)
`0xd31100` = D_ID fabric F_port
`00fffffe` = the S_ID
`0xd31100` = D_ID is the assignment of the Fabric address

Example Summary

Example 3 is the accept of FLOGI from the switch to the device (R_CTL=`0x23`, Extended Link Services Reply; D_ID=`0xd31100`, fabric F_port; S_ID=`0xfffffe`). The D_ID=`0xd31100` is the assignment of the Fabric address

Switch Fabric Internal Link Services (SW_ILS)

About Internal Link Services (ILS)

Internal Link Services refers to the service that allows a switch to communicate with itself. A Domain Controller (or embedded port) communicates to receive updated information.

When a `portlogdump` shows a Well Known Address communicating to another Well Known Address, refer to ILS for information about that communication. See "SW_ILS Examples" on page 414.

The SW_ILS section includes the following topics:

SW_ILS Command Codes

Table 66 explains the SW_ILS command codes.

Table 66: Switch Fabric Internal Link Services Command Codes

Code	Abbreviation	Description
0x01000000	IE_RJT	Reject
0x 02000000	IE_ACC	Inter Exchange Accept
0x 03000000	IE_ELOGI	Inter Exchange Element Login
0x 04000000	IE_LOGI	Inter Exchange Inter-Element Login
0x 05000000	IE_ELOGO	Inter Exchange Element Logout
0x 06000000	IE_LOGO	Inter Exchange Inter-Element Logout
0x 07000000	IE_DSP	Inter Exchange Distribute Service Parameters
0x 08000000	IE_VN	Inter Exchange Validate Name
0x 10000000	IE_ELP	Inter Exchange Exchange Link Parameters
0x11000000	IE_EFP	Inter Exchange Fabric Parameters
0x 12000000	IE_DIA	Inter Exchange Domain Identifier Assigned
0x 13000000	IE_RDI	Inter Exchange Request Domain ID

Table 66: Switch Fabric Internal Link Services Command Codes (Continued)

Code	Abbreviation	Description
0x 17000000	IE_BF	Inter Exchange Build Fabric
0x 18000000	IE_RCF	Inter Exchange Reconfigure Fabric
HP-Specific Command Codes		
0x 14000000	IE_HLO	Routing: Hello
0x 15000000	IE_LSU	Routing: Link State Update
0x 16000000	IE_LSA	Routing: Link State Ack
0x 19000000	IE_GAID	Get Alias ID
0x 1a000000	IE_RAID	Return Alias ID
0x 1b000000	IE_RSCN	Inter-switch RSCN
0x 1c000000	IE_INQ	Inquiry
0x 1d000000	IE_RTE	Interswitch Routing information
0x 1E000000	DRLIR	Disconnect Class 1 Connection
0x 20000000	DSCN	Disconnect Class 1 Connection
0x 21000000	LOOPD	Detect Queued Class 1 Connection Request Deadlock
0x 22000000	MR	Merge Request
0x 23000000	ACA	Acquire Change Authorization
0x 24000000	RCA	Release Change Authorization
0x 25000000	SFC	Stage Fabric Configuration
0x 26000000	UFC	Update Fabric Configuration
0x 3000xxxx	ESC	Exchange Switch Capabilities
0x70000000	IE_ZONE	Inter Exchange Zone Update (Vendor Unique)
0x71000000	IE_SGROUP	Inter Exchange Group wise commands
0x72000000	IE_SEC	Inter Exchange Security entry
0x73000000	IE_SLAPRequest	Inter Exchange SLAP Request
0x74000000	IE_SLAPAcknowledge	Inter Exchange SLAP Acknowledge
0x75000000	IE_SLAPConfirm	Inter Exchange SLAP Confirm
0x76000000	IE_SLAPDone	Inter Exchange SLAP Done
0x77000000	IE_SLAPReject	Inter Exchange SLAP Reject

Table 66: Switch Fabric Internal Link Services Command Codes (Continued)

Code	Abbreviation	Description
0x78000000	IE_RCS_INFO	Inter Exchange Reliable commit service info
0x79000000	IE_RCS_ACA	Inter Exchange RCS Acquire Change Authorization
0x7a000000	IE_RCS_SFC	Inter Exchange RCS Stage Fabric Config
0x7b000000	IE_RCS_UFC	Inter Exchange RCS Update Fabric Config
0x7c000000	IE_RCS_RCA	Inter Exchange RCS Release Change Authorization
0x7d000000	IE_RCS_TCO	Inter Exchange RCS Transfer Commit Ownership
0x7e000000	IE_RDTS	Inter Exchange RDTS Request
0x7f00000	IE_ECP	Inter Exchange Exchange credit parameters request
Trunking Support Code		
0x90000000	IE_EMT	Inter Exchange Read MARK timestamp(VU)
0x91000000	IE_ETP	Inter Exchange Exchange trunking parameter
External Link Services		
0x81000000	SW_RJT	Reject
0x82000000	SW_ACC	Accept
0x83000000	SW_CFN	Change Fabric Name
0x84000000	SW_WTV	Write Timeout Value
0x850000	SW_ON	Offline Notification

SW_ILS Reject Reason Codes (SW_RJT)

- To view a reject frame, see “SW_ILS Reject Frame” on page 485.
- To view a reject example, see “SW_ILS Reject Example” on page 418.

Table 67 specifies the SW_ILS reject reason codes.

Table 67: FC_SW Reject Reason Codes (SW_RJI)

Code	Abbreviation	Description
0x01	SW_INVALID_COMMAND	Invalid ELS Command Code – the command code is not recognized by the recipient.
0x02	SW_INVALID_VERSION	Invalid revision level. The recipient does not support the specified revision level.
0x03	SW_LOGICAL_ERROR	Logical Error – The request identified by the command code and the payload content is invalid or logically inconsistent for the conditions present.
0x04	SW_INVALID_IU_SIZE	Invalid payload size – The size of the payload is inconsistent with the command code and/or any length fields in the payload.
0x05	SW_LOGICAL_BUSY	Logical Busy – the port is unable to perform the request at this time. Busy reason explanation code: 01 – PHYSICAL_N_PORT_BUSY 03 – N_PORT_RESOURCE_BUSY
0x07	SW_PROTOCOL_ERROR	Protocol Error – an error has been detected that violates FC-2 protocols and is not covered by another reason code.
0x09	SW_CANT_PERFORM_REQ	Unable to perform command request – the recipient is unable to perform the request at this time.
0x0b	SW_NOT_SUPPORTED	Command not supported – the recipient does not support the ELS command.
Other value		Reserved.
0xff	SW_VENDOR_UNIQUE	Vendor-unique field indicates an error condition.

FC-SW (SW-RJT) Reject Reason Explanation Codes

Table 68 explains the FC-SW reason reject codes.

Table 68: FC-SW (SW-RJI) Reject Reason Explanation Codes

Code	Abbreviation	Explanation
0x00	SW_NO_EXPLANATION	No additional explanation
0x01	SW_CLASS_F_ERROR	Class F Service Parameter error
0x03	SW_CLASS_N_ERROR	Class N Service Parameter error
0x04	SW_UNKNOWN_CTL_MODE	Unknown Flow Control code
0x05	SW_UNKNOWN_CTL_PARAMS	Invalid Flow Control Parameters
0x0d	SW_INVALID_PORT_NAME	Invalid port name
0x0e	SW_INVALID_SWITCH_NAME	Invalid switch name
0x0f	SW_TOV_MISMATCH	R_A_TOV or E_D_TOV mismatch
0x10	SW_INVALID_DLIST	Invalid Domain_ID_List
0x19	SW_COMMAND_IN_PROGRESS	Command already in progress
0x29	SW_NO_MORE_RESOURCES	Insufficient resources available
0x2a	SW_NO_DOMAIN_ID	Domain_ID not available
0x2b	SW_INVALID_DOMAIN_ID	Invalid Domain ID
0x2c	SW_NON_SUPPORTED_REQ	Request not supported
0x2d	SW_NO_LINK_PARAMETERS	Link Parameters not yet established
0x2e	SW_NO_CONT_DOMAIN_IDS	Requested Domain_IDs not available
0x2f	SW_EPORT_ISOLATED	E_Port is Isolated
0x30	SW_CANT_TRUNK	Cannot trunk
0x3a	SW_EPORT_DISABLED	E port disabled
0x3b	SW_SLAP_NOTDONE	Slap not done
0x3c	SW_RDTS_NOTDONE	Zoning is not done
0x3d	SW_RDTS_NOTDONE	RDTS not done

SW_ILS Examples

The ILS examples below are explained in the following way:

- The first section (labeled **Example**) shows the whole example, and the subsequent sections are broken up line by line.
- Click on any colored link to go to related information.

For a text description of the events displayed in this example, see the Example Summary at the end of the example.

Routing Frame Example

Example

```
    time        task      event port cmd  args
-------------------------------------------------
1. 00:44:26.599  tFspf   Tx     8    40   02fffffd,00fffffd,0284ffff,14000000,10cac760
2. 00:44:26.599  tReceive Rx   8     0   c0fffffd,00fffffd,028400fb,         ,10cab4d0
```

Output Line 1

```
00:44:26.599  tFspf  Tx  8   40  02fffffd,00fffffd,0284ffff,14000000,10cac760
```

Table 69 explains the arguments in output line 1 of the example.

Table 69: Argument Breakdown for Example Line 1

Arg 1 02fffffd	Arg 2 00fffffd	Arg 3 0284ffff	Arg 4 14000000	Arg 5 10cac760
02 = RC_CTL (request)	00 = Identifier	0284 = OX_ID	14000000 = SW_ILS command code (routing Hello). "SW_ILS Command Codes" on page 409	10cac760 = IU address pointer
fffffd = D_ID (Fabric controller)	ffffd = S_ID (Fabric controller)	ffff = RX_ID		

Output Line 2

```
00:44:26.599  tReceive   Rx   8 0  c0fffffd,00fffffd,028400fb,         ,10cab4d0
```

Table 70 explains the arguments in output line 2 of the example.

Table 70: Argument Breakdown for Example Line 2

Argument 1 c0fffffd	Argument 2 00fffffd	Argument 3 028400fb	Argument 4 Null	Argument 5 10cab4d0
CO = RC_CTL (Link control acknowledged)	00 = Identifier	0284 = OX_ID	null = SW_ILS command code	10cab4d0 = IU address pointer (not available in v4.x). See "About the IU Pointer" on page 366.
fffffd = D_ID (Fabric controller)	ffffd = S_ID (Fabric controller)	00fb = RX_ID		

Example Summary

The Fabric Controller from one switch sends a handshake hello to the other Fabric Controller. The handshake is acknowledged.

Trunking Frame Example

Example

```
22:33:38.283  tFabric    Tx   3  84   02fffffd,00fffffd,02ceffff,9000005
22:33:38.283  tReceive   Rx   3  0    c0fffffd,00fffffd,02ce0089,         ,10cb1c40
22:33:38.283  tReceive   Rx   3  84   03fffffd,00fffffd,02ce0089,02000050,10cb2510
22:33:38.283  tTransmit  Tx   3   0   c0fffffd,00fffffd,02ce0089,         ,10cb2510
```

Output Line 1

```
22:33:38.283  tFabric   Tx   3  84  02fffffd,00fffffd,02ceffff,9000005
```

Table 71 explains the arguments in output line 1 of the example.

Table 71: Argument Breakdown for Example Line 1

Argument 1 02fffffd	Argument 2 00fffffd	Argument 3 02ceffff	Argument 4 9000005
02 = RC_CTL (request)	00 = Identifier	02ce = OX_ID	9000005 = Trunking IU Preamble
fffffd = D_ID	fffffd = S_ID	ffff = RX_ID	

Output Line 2

```
22:33:38.283  tReceive   Rx    3  0    c0fffffd,00fffffd,02ce0089,         ,10cb1c40
```

Table 72 explains the arguments in output line 2 of the example.

Table 72: Argument Breakdown for Example Line 2

Argument 1 c0fffffd	Argument 2 00fffffd	Argument 3 02ce0089	Argument 4	Argument 5 10cb1c40
CO = RC_CTL (Link control acknowledged)	00 = Identifier	02ce = OX_ID	null	10cb1c40 = IU address pointer
fffffd = D_ID	fffffd = S_ID	ffff = RX_ID		

Output Line 3

```
22:33:38.283  tReceive   Rx    3  84   03fffffd,00fffffd,02ce0089,02000050,10cb2510510
```

Table 73 explains the arguments in output line 3 of the example.

Table 73: Argument Breakdown for Example Line 3

Argument 1 03fffffd	Argument 2 00fffffd	Argument 3 02ce0089	Argument 4 02000050	Argument 5 10cb2510510
03 = RC_CTL (reply)	00 = Identifier	02ce = OX_ID	02 = (Accept)	10cb2510 = IU address pointer
fffffd = D_ID (Fabric controller)	fffffd = S_ID (Fabric controller)	0089 = RX_ID	000050 =	

Output Line 4

```
22:33:38.283  tTransmit  Tx    3   0   c0fffffd,00fffffd,02ce0089,         ,10cb2510
```

Table 74 explains the arguments in output line 4 of the example.

Table 74: Argument Breakdown for Example Line 4

Argument 1 c0fffffd	Argument 2 00fffffd	Argument 3 02ce0089	Argument 4	Argument 5 10cb2510
`0c` = RC_CTL (link control acknowledge)	`00` = Identifier	`02ce` = OX_ID	null	`10cb2510` = IU address pointer
`fffffd` = D_ID (Fabric controller)	`fffffd` = S_ID (Fabric controller)	`0089` = RX_ID		

Example Summary

The Fabric Controller on one switch sends a trunking stamp to the other switch's Fabric controller. The Request is acknowledged and accepted.

NSD Example

Example

```
16:09:052.553 nsd   rscn     0fffc09 00fffc0a, 1b000000, 500a1f00,000000001
```

General Information

- R_CTL = 02 for all request frames, and 03 for all reply frames.
- CS_CTL = 00. Otherwise, see IU_Status codes.
- D_ID and S_ID are set as indicated for the specific SW_ILS, FFFFFD or FFFCxx (FFFCxx, xx= domain ID).

Example Summary

The example above shows S_ID domain controller (fffc0a) talking to D_ID domain controller (fffc09); they are communicating an HP Specific Interswitch RSCN code (see “Specific Codes” on page 382).

SW_ILS Reject Example

The following example focuses mainly on reading the areas that affect the reject response.

Example

```
11:01:10.716  tFspf     Tx       2   40 02fffffd,00fffffd,01abffff,14000000,11cdde90
11:01:10.949  tShell   ioctl    2   dd  101f24c0,0* 2
11:01:11.916  tShell    ioctl    3   dd  101f24c0,0* 2
11:01:12.499  tReceive  Rx3      2    0  81140500,00240300,074bffff,        ,11cd35a0
11:01:12.499  tReceive  reject   2       16
```

Table 75 provides descriptions of the SW_ILS reject example.

Table 75: SW_ILS Reject Example Descriptions

Entry	Description	Cross-Reference
tFspf	A Fibre Channel Shortest Path First (FSFP) routing Task.	See "Task" on page 359.
14000000	An ILS (hello) transmission.	See "Switch Fabric Internal Link Services (SW_ILS)" on page 409.
tShell	A Shell Task, which is a Telnet task that starts up a shell in VX works.	See "Task Descriptions" on page 360.
ioctl	An I/O Control event.	See "I/O Control (ioctl)" on page 388.
f2	Specific IOCTL code that displays the number of filter hit count.	See "IOCTL CTL Codes" on page 388.
reject	Reject event.	See "FC_SW Reject Reason Codes (SW_RJI)" on page 412 and "FC-SW (SW-RJI) Reject Reason Explanation Codes" on page 413

Zoning Codes (NZ)

Zoning Request Codes

Table 76 describes the zoning request codes

Table 76: Zoning Request Codes for Zoning Exchange

Code	Abbreviation	Description
0x22000000	IE_NZ_MR	
0x23000000	IE_NZ_ACA	
0x24000000	IE_NZ_RCA	
0x25000000	IE_NZ_SFC	
0x26000000	IE_NZ_UFC	
0x70000000	IE_ZONE	Zone Update (Vendor Unique)
0x71000000	IE_SGROUP	Group wise commands
0x72000000	IE_SEC	Security entry
0x73000000	IE_SLAPRequest	SLAP Request
0x74000000	IE_SLAPAcknowledge	SLAP Acknowledge
0x75000000	IE_SLAPConfirm	SLAP Confirm
0x76000000	IE_SLAPDone	SLAP Done
0x77000000	IE_SLAPReject	SLAP Reject
0x78000000	IE_RCS_INFO	Reliable commit service info
0x79000000	IE_RCS_ACA	RCS Acquire Change Authorization
0x7a000000	IE_RCS_SFC	RCS Stage Fabric Config
0x7b000000	IE_RCS_UFC	RCS Update Fabric Config
0x7c000000	IE_RCS_RCA	RCS Release Change Authorization
0x7d000000	IE_RCS_TCO	RCS Transfer Commit Ownership
0x7e000000	IE_RDTS	RDTS Request
0x7f000000	IE_ECP	Exchange credit parameters request
Trunking support code		
0x90000000	IE_EMT	Read MARK timestamp(VU)
0x91000000	IE_ETP	Exchange trunking parameter

Table 76: Zoning Request Codes for Zoning Exchange (Continued)

Code	Abbreviation	Description
External Link Services		
0x81000000	SW_RJT	Reject
0x82000000	SW_ACC	Accept
0x83000000	SW_CFN	Change Fabric Name
0x84000000	SW_WTV	Write Timeout Value
0x85000000	SW_ON	Offline Notification

Zoning Request Response Codes

Table 77 describes the zoning request response codes.

Table 77: Zoning Request Response Codes

Code	Description
0x00	NZ_SUCCESSFUL
0x01	NZ_FABRIC_BUSY
0x02	NZ_FAILED
(0 - 100)	NZ_ERROR_BASE

Zoning Reason Codes

Table 78 lists the zoning reason codes.

Table 78: Zoning Reason Codes

Code	Reason
0x00	NZ_NO_REASON
0x01	NZ_INVALID_DATA_LEN
0x02	NZ_UNSUPPORTED_CMD
0x04	NZ_NOT_AUTHORIZED
0x05	NZ_INVALID_REQUEST
0x06	NZ_FABRIC_CHANGING
0x07	NZ_UPDATE_NOT_STAGED

Table 78: Zoning Reason Codes

Code	Reason
0x09	NZ_INVALID_DATA
0x0a	NZ_CANNOT_MERGE
0x0b	ZONING_NO_LICENSE

TZone Request Codes

TZone - New Zoning SFC Request's Operation Request Values.

R_CTL = 22 and 22
Payload word 0 = zoning request value

Table 79 describes the new zoning request operation request values.

Table 79: TZone - New Zoning SFC Request's Operation Request Values

Zoning Request Value	Description
0x03	NZ_ACTIVATE_ZONESET
0x04	NZ_DEACTIVATE_ZONESET
0xF0 Vendor-unique fabric configuration server (FCS) request operation code used for saving configuration without activating or deactivating.	NZ_SAVE_FULLZONESET

Zoning Transaction Abort Reason Codes

Table 80 specifies the zoning abort reason codes.

Table 80: Zoning Transaction Abort Reason Codes

Code	Description
0xa0	ERR_ZONE_MERGE_RECEIVED
0xa1	ERR_ZONE_CONFIG_CHANGE
0xa2	ERR_ZONE_BAD_CONFIG
0xa3	ERR_ZONE_OP_FAILED
0xa4	ERR_ZONE_CANNOT_START_TRANSACTION

Table 80: Zoning Transaction Abort Reason Codes

Code	Description
0xa5	ERR_ZONE_SHELL_EXITED
0xa6	ERR_ZONE_NOT_OWNER
0xa7	ERR_ZONE_VALIDATION_FAILED

Zoning Specific Opcodes

SW_ILS (0x7f) ENT_MEMBER - Type of Zoning Members

Table 81 describes the zoning-specific operation codes.

Table 81: Zoning Specific Opcode

Code	Type	Description
SW_ILS (0x7f) ENT_MEMBER - Type of Zoning Members		
0x01	PORT	Entry describes physical port
0x02	ENT_WWN	Entry describes WWN
0x04	ENT_BMAP	Entry describes al_pa bitmap
0x08	ENT_NAME	Entry describes a name
SW_ILS (0x80) “ENT_LUN” – LUN information in entry_t valid		
0x01	ENT_TARGET	e_devType is TARGET
0x02	ENT_INITIATOR	e_devType is INITIATOR

Zone Configuration Operations Codes

Table 82 specifies the operations.

Table 82: Zone Configuration Operations

Code (hex)	Operation	Description
00000001	CREATE	Create an object
00000002	DELETE	Delete an object
00000003	ADD	Add a member to an object
00000004	REMOVE	Remove a member from an object
00000005	CLEAR	Clear all objects
00000006	DISABLE	Disable configuration

Table 82: Zone Configuration Operations

Code (hex)	Operation	Description
00000007	ENABLE	Enable configuration
00000008	SAVE	Save in flash memory
00000009	MERGE	Merge two configurations
0000000A	REMOTE	Look up ID on remote switch
0000000B	CHECK	Checksum configuration

Zone Object Code Types

Table 83 shows the zone object types.

Table 83: Zone Object Types

Code (hex)	Description
00	Name Zoning
01	Zone set (Cfg)
02	Zone
03	Zone Alias
04	QLP
05	Cfg_end
06	IPO
07	Enable_cfg
08	Active_cfg

Zone Error (tzone-reject) Code

Table 84 describes the zone error codes.

Table 84: Zone Error (tzone-reject) Code

Hexadecimal	Abbreviation	Description
0	NOERROR	Generic - no error
1	NOMEMORY	Generic malloc failure
2	ZONE RULE CHECK ERROR CODE EZACCEPT	No zoning rule violation
3	EZBADPORT	Non-existent port number

Table 84: Zone Error (tzone-reject) Code (Continued)

Hexadecimal	Abbreviation	Description
4	FCTYPEMIX	Specific FC type and wildcard mix
5	ERSINGLEDEV	More than one dev when LUN presents
6	EZLUNMIX	Mixture of devices w/ and w/o LUN at the same port
7	EZMENMIX	Mix of port and WWN zone members
8	EZHARDSOFTMIX	Mix of hard and soft zones
9	EZFAQLMIX	Mixing hard zoning with FA or QL zone
A	EZLUNMENMIX	Mix of QQQ
B	ZONE TYPE MANAGEMENT ERROR CODE ZT_SOFTZONE	Soft zoning - no need for ZT
C	ZT_FABASSIST	FA zone - no need for ZT
E	ZT_DRIVERERR	Driver returns error
F	ZG_NO_MORE_CAM	No more CAM entry in port driver
10	ZCHECKBADWWN	Zone check bad WWN authentication
11	WWN_IN_PORTZONE	WWN device in hard PORT zone
12	OFFSET_MASK_FULL	No offset register available
13	PORT_EPORT	Port is an E-port

Zone Example

FC-4 Type Device Data - Zoning Request

Example

```
22:48:10.633 tReceive   Rx 8 4  02fffc0b,00fffc0a,0053ffff,70846400,10d065f0
22:48:10.633 tTransmit  Tx 8 0  c0fffc0a,00fffc0b,00530235, ,10d065f0
22:48:10.633 tSwitch    Tx 8 4  03fffc0a,00fffc0b,00530235,02840000,10d065f0
22:48:10.633 tReceive   Rx 8 0  c0fffc0b,00fffc0a,00530235, ,10d065f0
```

Output Line 1

```
22:48:10.633 tReceive Rx 8 4 02fffc0b,00fffc0a,0053ffff,70846400,10d065f0
```

Table 85 explains the arguments in line one of the output.

Table 85: Breakdown of Argument Fields in Output Line 1

Argument 1 02fffc0b	Argument 2 00fffc0a	Argument 3 0053ffff	Argument 4 70846400	Argument 5 10d065f0
02 = RC_CTL (request)	00 = Identifier	0053 = OX_ID	Zoning IU Preamble: 70 = IE_ELSCode (zoning) 84 = New zoning revision (>2.3v firmware) 00 = Zone Object Type (Name zoning)	10d065f0 = IU address pointer
fffc0b = D_ID	fffc0a = S_ID	ffff = RX_ID		

Output Line 2

```
22:48:10.633 tTransmit Tx 8 0 c0fffc0a,00fffc0b,00530235, ,10d065f0
```

Table 86 explains the arguments in line 2 of the output.

Table 86: Breakdown of Argument Fields in Output Line 2

Argument 1 c0fffc0a	Argument 2 00fffc0b	Argument 3 00530235	Argument 4	Argument 5 10d065f0
C0 = RC_CTL (Link control acknowledge)	00 = Identifier	0053 = OX_ID	SW_ILS command code = null	10d065f0 = IU address pointer
fffc0a = D_ID	fffc0b = S_ID	0235 = RX_ID		

Output Line 3

```
22:48:10.633 tSwitch Tx 8 4 03fffc0a,00fffc0b,00530235,02840000,10d065f0
```

.Table 87 explains the arguments in line 3 of the output.

Table 87: Breakdown of Argument Fields in Output Line 3

Argument 1 03fffc0a	Argument 2 00fffc0b	Argument 3 00530235	Argument 4 02840000	Argument 5 10d065f0
03 = RC_CTL (reply)	00 = Identifier	00530 = OX_ID	02 = Zoning IU preamble (accept)	10d065f0 = IU address pointer
fffc0a = D_ID	fffc0b = S_ID	0235 = RX_ID	84 = New zoning revision (>2.3v firmware)	

Output Line 4:

```
22:48:10.633 tReceive Rx 8 0 c0fffc0b,00fffc0a,00530235, ,10d065f0
```

Table 88 explains the arguments in line 4 of the output.

Table 88: Breakdown of Argument Fields in Output Line 4

Argument 1 c0fffc0b	Argument 2 00fffc0a	Argument 3 00530235	Argument 4	Argument 5 10d065f0
c0 = RC_CTL (Link control acknowledge)	00 = Identifier	0053 = OX_ID	SW_ISL command code = null	10d065f0 = IU address pointer
fffc0b = D_ID	fffc0a = S_ID	0235 = RX_ID		

Example Summary:

Embedded port `fffc0a` sends zoning code `70` request to other embedded port `fffc0b`. Embedded port `fffc0b` sends a link control acknowledgment.

About FSS

The primary function of FSS is to deliver State Update messages from active components to their peer standby components. FSS determines if fabric elements are synchronized (and are thus FSS compliant).

A Fabric OS switch service is composed of a set of components, which are either a user-space service daemon or a kernel-space driver, with a symbolic name to identify its function inside the switch service and the instance number of the switch that the component is operating on.

FSS monitors the Fabric OS elements (ASIC driver, ns, zone, web, fabric, fspf, ms, ps, and so forth) and reports them either FSS compliant or not FSS compliant. A Fabric Service is deemed fault resilient (or FSS compliant) if a set of its components is operating in an active standby mode, and the state replication is carried out from the active components to their corresponding standbys.

To learn to read an FSS entry in the `portlogdump`, see "FSS Example" on page 431.

FSS Fields in the portlogdump Output

Each line of FSS output in the `portlogdump` consists of the fields shown in Table 89.

Table 89: FSS Field Descriptions

Time	Task	Event	Port	Cmd	Argument
Displays time of event	Always FSSk	Can be msg, event, or cmd. See "FSS Messages" on page 428.	Always "0" (FSS is not related to CPs, not ports).	0 = Sent, or Transmitted (TX). 1 = Received (RX).	Argument1 = service ID and component ID. See "FSSk Service Identification" on page 430 and "FSSk Component Identification" on page 430.
					Argument2 = send/receive operation data.
					Argument3 = Optional Flags
					Argument4 = a text description. See "FSS Messages" on page 428.

FSS Messages

The information below refers to the relationship between the event column and the final entry of the Argument column. Use Table 90 to decode a specific Event and Argument entry.

```
time          task       event  port cmd  args
-------------------------------------------------
21:54:04.763  FSSK       event    0    0 00000000,00000000,00000005,TRAC
```

Table 90: FSS Messages

Event Type	4th Argument Abbreviation	Description
msg	EXCH	Broadcast message exchange well known address
msg	UPDA	Message state update.
msg	ACK	Message - state acknowledgment.
msg	STAR	Message - sync started.
msg	STOP	Message - sync stopped.
msg	RECO	Message - recover.
msg	YIEL	Message -
msg	NONE	Message - no message.
msg	TAKE	Message - Standby take control.
msg	TEST	Message - Test Point.
event	STAR	Sync start event.
event	UPCO	Up connection event.
event	DOWN	Down connection event.
event	COMP	Image complete event.
event	INCO	Incomplete incomplete event.
event	DUMP	A dump is ready.
event	NONE	No event occurred.
event	SYNC	Sync success event.
event	FAIL	Sync failure event.
event	STOP	Sync stopped.

Table 90: FSS Messages (Continued)

Event Type	4th Argument Abbreviation	Description
event	RECO	The recovery failed.
event	TAKE	A take control event occurred.
event	YIEL	A yield control event occurred.
event	MISM	A mismatch event occurred.
event	UPDA	A state update event occurred.
event	ACTI	Event reported. The active CP is ready.
event	STAN	Event reported. The standby CP is ready.
event	TXQH	Event reported. Transmissions are high.
event	RXQH	Event reported. Receptions are high.
event	MISS	Event reported. A service is missing.
event	AVAI	Event reported. Service is available.
event	TRAC	A trace of events was run.
cmd	NONE	No command.
cmd	STAR	The sync started.
cmd	STOP	The sync stopped.
cmd	YIEL	Yield control.
cmd	TAKE	Take Control.
cmd	RESE	Reset.
cmd	FREE	Freeze.
cmd	UNFR	Unfreeze.
cmd	UPDA	State update.
cmd	CONN	Connect.

FSSk Service Identification

The Service ID is displayed in the first 4 bits of Argument 1.

```
21:54:04.882  FSSK       event    0    0 00020000,00000000,00000000,UPCO
```

The Service ID can be viewed by running the `hadump` command.

Example Output From the hadump Command

```
=== FSS Service Dump : fcsw0 ===
== State ==
fcsw0(2): ACTIVE(0), Required-------------------------> **service ID 2
local = IMG_COMP, prev = IMG_NONE, peer = IMG_NONE
     Name       Local           Remote
     fcsw0(M)   IMG_COMP        IMG_INCOMP---------------> component id 0
       swc(M)   IMG_COMP        IMG_INCOMP---------------> component id 1
       fcp(M)   IMG_COMP        IMG_INCOMP---------------> component id 2
        rt(M)   IMG_COMP        IMG_INCOMP
```

FSSk Component Identification

A list of possible components can be found by using the `hadump` command. Table 91 lists the component names and their associated IDs.

The Component ID# appears in the 2nd bit of Argument 1.Use that number to determine the component that is being referenced.

```
22:15:51.430  FSSK       msg      0    1 00020001,00000000,00000014,UPDA
```

Table 91: FSSk Component Identification

Component ID	Component Name
0x0	fcsw
0x1	swc
0x2	fcp
0x3	rt
0x4	fc
0x5	fabric
0x6	zone
0x7	fspf

Table 91: FSSk Component Identification (Continued)

Component ID	Component Name
0x8	ns
0x9	ms
0xA	ps
0xB	rcs
0xC	evm
0xD	track
0xE	ts
0xF	slap
0x10	security
0x11	web
0x12	snmp
0x13	fw
0x14	diagfss

FSS Example

Reading FSSK Output in the portlogdump

Example

```
time           task       event  port  cmd args
-------------------------------------------------
18:13:37.979   FSSK       msg       0     0 0002000e,0000012c,00000000,UPDA
18:13:56.584   FSSK       cmd       0     0 00000000,00000000,00000000,STOP
18:13:56.584   FSSK       event     0     0 00000000,00000000,00000000,STOP
18:13:56.584   FSSK       msg       0     0 00000000,00000005,00000000,UPDA
18:13:56.861   FSSK       cmd       0     0 00020000,00000000,00000000,STOP
18:13:56.862   FSSK       event     0     0 00020000,00000000,00000000,STOP
18:13:56.862   FSSK       msg       0     0 00020000,00000005,00000000,UPDA
18:13:56.874   FSSK       cmd       0     0 00040000,00000000,00000000,STOP
18:13:56.875   FSSK       event     0     0 00040000,00000000,00000000,STOP
```

Follow the steps below to read the example above from left to right:

1. The `task` column should display `FSSK`. See “About FSS” on page 426 for the FSS description.
2. Look at the `event` column. All events (`msg`, `cmd`, `event`, and so forth) are described in “FSS Field Descriptions” on page 427.
3. Bypass the `port` column; it is always `0,` since FSS is not a port-related service.
4. Look at the `cmd` column.
   - `0` indicates Sent, or Transmitted (TX).
   - `1` indicates Received (RX).
5. Begin reading the **args** column.
   - Argument1 (the first 8 bits) displays the Service ID and the Component ID. See the “FSSk Component Identification” on page 430.
   - Argument2 (the second 8 bits) displays send/receive operation data.
   - Argument3 (the third 8 bit set) displays optional flags (send/receive data).
   - Argument4 (the fourth entry), displays text that helps clarify the output.
     - Note the displayed text (for example, `UPDA`).
     - Look back at the `event` column. You see, for example `msg`.
     - Use “FSS Field Descriptions” on page 427 to find the message description.
       For example: Find *msg* ----> UPDA ---> read description.

Fabric Services

About Fabric Services

Fabric Services refers to communication to and from any Well-Known Address. Fabric Services response codes, reason codes, and explanations are described in Table 92, Table 93, and Table 94, respectively.

Table 92: Fabric Services Response Command Codes

Code	Abbreviation	Description
0x01000000	FS_RJT	Reject
0x02000000	FS_ACC	Accept
0x03000000	FS_INQ	Vendor inquiry data
0x04000000	FS_FADDQ	Fabric address query
0x05000000	FS_FTOPO	Fabric topology

Table 93: Fabric Services Reject Reason Codes

Code	Description
0x01	FS_INVALID_COMMAND
0x03	FS_LOGICAL_ERROR
0x09	FS_CANT_PERFORM_REQ
0x01	FS_INVALID_COMMAND

Table 94: Fabric Services Reject Reason Code Explanation

Code	Description
0x00	ASRJT_EXPL_NONE
0x30	ASRJT_EXPL_NOSUCHALIAS
0x31	ASRJT_EXPL_NORESOURCE
0x32	ASRJT_EXPL_INVALID_ALIAS_ID
0x33	ASRJT_EXPL_ALIAS_ID_NOEXIST
0x34	ASRJT_EXPL_RESOURCE_PROBLEM
0x35	ASRJT_EXPL_SPAR_CONFLICT
0x36	ASRJT_EXPL_ALIAS_TOKEN_INVALID
0x37	ASRJT_EXPL_ALIAS_TOKEN_NOTSUPP
0x38	ASRJT_EXPL_CANTFORM_PORTLIST
0x40	ASRJT_EXPL_CANTFORM_CLASS

Table 94: Fabric Services Reject Reason Code Explanation (Continued)

Code	Description
0x41	ASRJT_EXPL_NOSUCH_TOKEN
0x42	ASRJT_EXPL_UNAUTHREQ_BADPASSWD
0x43	ASRJT_EXPL_UNAUTHREQ_BADAUTH
0x44	ASRJT_EXPL_INVALID_AUTH_CTL

Table 95 provides segmentation reason details.

Table 95: Fabric Segmentation Reason Details for Port

Error	Reason
FAB_SEG_INCOMPAT_UNKNOWN	Unknown reason
FAB_SEG_INCOMPAT_VERSION	Version mismatch
FAB_SEG_INCOMPAT_FCTL_LEN	Flow Control len mismatch
FAB_SEG_INCOMPAT_FCTL_MODE	Flow control invalid mode
FAB_SEG_INCOMPAT_STRUCT_SZ	Passed size > fabOP_t
FAB_SEG_INCOMPAT_BB_CREDIT	BB credit mismatch
FAB_SEG_INCOMPAT_DFSZ	recv DataField sz mismatch
FAB_SEG_INCOMPAT_RATOV	RA TOV mismatch
FAB_SEG_INCOMPAT_EDTOV	ED TOV mismatch
FAB_SEG_INCOMPAT_OPMODE	Op Mode mismatch
FAB_SEG_INCOMPAT_LINK_CTL	Link Ctrl mismatch
FAB_SEG_INCOMPAT_CLASS2	Class 2 mismatch
FAB_SEG_INCOMPAT_CLASS3	Class 3 mismatch
FAB_SEG_INCOMPAT_MULCAST	Multicast mismatch
FAB_SEG_INCOMPAT_VCCONFIG	VC config mismatch
FAB_SEG_INCOMPAT_PIDMAP	VC PID MAP mismatch
FAB_SEG_INCOMPAT_CLASS1_SZ	Class1 datasize mismatch
FAB_SEG_INCOMPAT_CLASS1_OPT	Class1 options mismatch
FAB_SEG_INCOMPAT_CLASS2_SZ	Class2 datasize mismatch
FAB_SEG_INCOMPAT_CLASS2_OPT	Class2 options mismatch
FAB_SEG_INCOMPAT_CLASS3_SZ	Class3 datasize mismatch

Table 95: Fabric Segmentation Reason Details for Port (Continued)

Error	Reason
FAB_SEG_INCOMPAT_CLASS3_OPT	Class3 options mismatch
FAB_SEG_INCOMPAT_CLASSF_OPT	ClassF options mismatch
FAB_SEG_INCOMPAT_CLASSF_INITCTL	ClassF init ctl mismatch
FAB_SEG_INCOMPAT_CLASSF_RECCTL	ClassF rec ctl mismatch
FAB_SEG_INCOMPAT_CLASSF_SZ	ClassF data sz mismatch
FAB_SEG_INCOMPAT_CLASSF_CONSE	ClassF con seq mismatch
FAB_SEG_INCOMPAT_CLASSF_EECRE	ClassF EE Credit mismatch
FAB_SEG_INCOMPAT_CLASSF_OPNSE	ClassF OPN SEQ mismatch
FAB_SEG_INCOMPAT_CLASSF_RSVD	ClassF resvd mismatch
FAB_SEG_INCOMPAT_MAX_DET_REASON	Maximum reasons

ISL Miscellaneous

Table 96 shows the ISL flow control values.

Table 96: ISL Flow Control Values

Value	Description
hex 0001	Vendor Unique
hex 0002	R_RDY Flow Control
hex 0003 - FFFE	Vendor Unique
Other Values	Reserved

Table 97 shows the ISL flow control parameters

Table 97: ISL Flow Control Parameters

Size	Item
4	BB_Credit
16	Compatibility Parameters

Table 98 shows the switch priority field values.

Table 98: Switch Priority Field Values

Hexadecimal Value	Description
00	Reserved
01	Highest priority value. (Note 1)
02	The switch was the principal switch prior to sending or receiving BF. (Note 2)
03 to FE	Higher to lower priority values. (Note 3)
FF	The switch is not capable of acting as a principal switch.
Notes - 1. This value allows the system administrator to establish which switch becomes the principal switch. 2. This allows the same switch to become principal switch if it is still part of the Fabric after sending and/or receiving the Build Fabric SW_ILS. 3. The Switch_Priority value for a given switch is established by means not defined by this standard.	

Fibre Channel Common Transport Protocol (FC-CT)

The FC Common Transport Protocol section includes the following:

Name Server Information

Management Server Information

Zoning Information

Alias Service Information

Example

About FC Common Transport Protocols (FC-CT)

The Fibre Channel Common Transport Protocol is used when accessing the following generic service provisions:

- Name Server (FFFFFC)
- Time Sever (FFFFFB)
- Management Sever (FFFFFA)
- Alias Server (FFFFF8)
- Security-Key Distribution Service (FFFFF7).

The N_port uses FC-4 Data Device Frames to perform the request service or query function to these generic services. The R_CTL field of FC-4 Data Device request is always set to 0x02, and the R_CTL field of the reply is set to 0x03. The type field for both requests and replies is 0x20 (`portlogdump` trace does not provide the Type field information). The command code for FC-4 Data Device is always the third word of the payload (word 8) for both the request and reply.

There are 2148 bytes in a frame; `portlogdump` captures only a portion of the frame.

For Tx and Rx events, the first Argument field obtains the portion of the header and one word of the payload, word6. Arguments 1, 2 and 3 belong to the FC_PH header (word 0,1,4 = R_CTL,D_ID,S_ID,OX_ID,RX_ID). The last argument (4th argument) belongs to the payload. More payload data obtains in the ctin and ctout events.

Table 99 describes the FC-CT Frame.

Table 99: FC-CT Frame

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
HEADER	R_CTL =02 or 03	D_ID		
	CS_CTL=00	S_ID		
	Type =20	F_CTL		
	SEQ_ID	DF_CTL	SEQ_DNT	
	OX_ID		RX_ID	
5	**Parameter**			
6	**FC-CT Header Usage**			

Table 100 specifies FC-CT header usage.

Table 100: Type of FC-CT Header Usage

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0-3	Basic CT_IU preamble			
4-25	Extended CT_IU preamble			

Basic CT_IU Preamble

Note: This reference covers only the Basic CT-IU Preamble.

Table 101 explains the bits in the CT-IU preamble.

Table 101: Basic CT_IU Preamble

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
6	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT)		
7	GS_TYPE	GS_Subtype	Options	Reserved
8	Command/Response Code page 432		Maximum/Residual Size	
9	Reserved	Reason Code	Reason Code Explanation	Vendor Unique

FC-CT Definitions

CT_Rev

Denotes the revision of the protocol. A version of hex ‘01’ indicates prior versions of this standard. A value of hex’02’ should be used to indicate GS3.rev7.01.

Note: The version was changed to hexadecimal 02 to allow implementations to indicate support of the extended CT_IU preamble and the partial response indicator.

IN_ID

This field is set to zero by the Requesting_CT.

Note: The IN_ID field is provided to allow distributed servers to communicate the identity of the original requestor. This field is not intended to enable third-party responses by distributed servers.

GS_Type

GS_Type is used to identify the type of Fibre Channel service (see Table 102).

Table 102: GS_Type Values

Value	Service
00-1F	Vendor Unique
20	Reserve for us FC-SW2
FF	Broadcast
FE	Fabric_F_Port
FD	Fabric Controller
FC	Name Server
FB	Time Server
FA	Management Server
F9	QOS Provider
F8	Alias Server
F7	Key Services

GS_Subtype

This field indicates the specific Server behind the Service. Values in this field are provided by the individual Service.

The GS_Subtype field is used to indicate second level routing behind the N_ Port. For example, if more than one server is provided by the Directory Service at the well-known address hex 'FFFFFC, the GS_Subtype field is used to distinguish these different servers.

See Table 111 on page 450 and Table 116 and page 460.

About the Command Response Code Field

The Command Response field indicates whether the CT_IU is a request or a response. If the CT_IU is a request, this field specifies the command to be performed. If the CT_IU is a response, this field indicates whether the request was accepted or rejected. Requests and responses are further described in the Name

Server and Management Server tables (“Name Server Commands and Code Descriptions” on page 441 and “Management Server Command Codes” on page 454). Table 104 provides the valid command response code values.

There are 2148 bytes in a frame. However, the `portlogdump` captures only a portion of the frame.

For Tx and Rx events:

- The first `Argument` field obtains the portion of the header and one word of the payload, word6.
- `Arguments` 1, 2 and 3 belong to the FC_PH header (word 0,1,4 = R_CTL, D_ID, S_ID, OX_ID, RX_ID).
- The last argument (4th argument) belongs to the payload. More payload information is obtained in the `ctin` and `ctout` events.

About the Name Server (SNS)

The Name Server (also referred to as the *Simple Name Server*) is a switch service that stores names, addresses, and attributes, and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a Well-Known Address. It may also be referred to as *directory service*.

The following topics are discussed in this section:

Name Server Commands and Code Descriptions

Table 103 explains the Name Server command codes.

Table 103: Name Server Command Codes

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
Query with port ID				
0100	GA_NXT	Get all next	Port Identifier	All
0101	GID_A	Get identifiers	List of Domain_IDs or Domain_ID/Area_IDs.	List of Domain_IDs or Domain_ID/Area_IDs.
0112	GPN_ID	Get Port Name	Port Identifier is hex (Note that the null value for the Port or Node Name object is hex '00 00 00 00 00 00 00'.)	Port Name (Note that the null value for the Port or Node Name object is hex '00 00 00 00 00 00 00 00'.)
0113	GNN_ID	Get Node Name	Port Identifier	Node Name
0114	GCS_ID	Get Class of Service	Port Identifier	Class of Service
0117	GFT_ID	Get FC_4 Types	Port Identifier	FC-4 Types
0118	GSPN_ID	Get Symbolic Port Name	Port Identifier	Symbolic Port Name
011A	GPT_ID	Get Port Type	Port Identifier	Port Type
011B	GIPP_ID	Get IP Address (Port)	Port Identifier	IP Address (Port)
IP Address (Port)	GFPN_ID	Get Fabric Port Name	Port Identifier	Fabric Port Name
011D	GHA_ID	Get Hard Address	Port Identifier	Hard Address
011E	GFD_ID	Get FC-4 Descriptors	Port Identifier	List of FC-4 Descriptors
011F	GFF_ID	Get FC-4 Features	Port Identifier	FC-4 Features
Query with Port name				
0121	GID_PN	Get Port Identifiers	Port Name	Port Identifier
012B	GIPP_PN	Get IP Address (Port)	Port Name	IP Address (Port)
Query With Node Name				
0131	GID_NN	Get Port Node Name	Node Identifiers	List of Port Identifiers

Table 103: Name Server Command Codes (Continued)

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
0132	GPN_NN	Get Port Node Names	Node Name	List of Port Identifiers and Port Names
0135	GIP_NN	Get IP Address (Node)	Node Name	IP Address (Node)
0136	GIPA_NN	Get Initial Process Associator	Node name	Initial Process Associator
0139	GSNN_NN	Get Symbolic Node Name	Node Name	Symbolic Node
Query With IP				
0153	GNN_IP	Get Node Name	IP Address (Node)	Node Name
0156	GIPA_IP	Get Initial Process Associator	IP Address (Node)	Initial Process Associator
0171	GID_FT	Get Port Identifiers	None, because FC-4 Type is specified as an encoded value, not as an object.	List of List of Port Identifiers.
0172	GPN_FT	Get FC4-Type Port Name	None, because type is specified as an encoded value, not as an object.	List of port identifiers and port names.
0173	GNN_FT	Get FC-4 Type Node Names		List of port identifiers and port names.
Query With Port Type				
01A1	GID_PT	Get Port Identifiers	Port Type (see "Name Server Port Types" on page 450)	List of Port Identifiers
Query With IP Port				
01B1	GID_IPP	Get Port Identifiers for IP Address (Port)	IP Address (Port)	List of Port Identifiers
01B2	GPN_IPP	Get Port Name	IP Address (Port)	Port Name
Query With FC-4 Features				
01F1	GID_FF	Get Port Identifiers	FC-4 Features	List of Port Identifiers
Registration				
0212	RPN_ID	Register Port Name	Port Identifier, Port Name	None

Table 103: Name Server Command Codes (Continued)

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
0213	RNN_ID	Register Node Name	Port Identifier, Node Name	None
0214	RCS_ID	Register Class of Service	Port Identifier, Class	None
0217	RFT_ID	Register FC-4 Types	Port Identifier, FC-4 Types	None
0218	RSPN_ID	Register Port SymbolicName for this Port ID	Port Identifier, Symbolic Port Name	None
021A	RPT_ID	Register Port Type for this Port ID	Port Identifier, IP Address (Port)	None
021B	RIPP_ID	Register IP Address (Port)	Port Identifier, IP Address (Port)	None
021C	RFPN_ID	Register Fabric Port Name	Port Identifier, Fabric Port Name	None
021D	RHA_ID	Register Hard Address	Port Identifier, Hard Address	None
021E	RFD_ID	Register FC-4 Descriptors	Port Identifier, FC-4 Types and FC-4 Descriptors	None
021F	RFF_ID	Register FC-4 Features	Port Identifier, FC-4 Features	None
0235	RIP_NN	Register IP Address for this Node WWN	Node Name, IP Address (Node)	None
0236	RIPA_NN	Register IP Address for this Node WWN	Node Name, Initial Process Associator	None
0239	RSNN_NN	Register Node Symbolic Name for this Node WWN	Node Name, Symbolic Node Name	None

Table 103: Name Server Command Codes (Continued)

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
De-Registration				
0300	DA_ID	De-register all	Port Identifier	None
FC_CT Command Restrictions The following command codes are not used by any Well-known Server for the FC-GS-x client/server interface: Command codes 0400-04FF and E000-EFFF: Fabric internal FC-CT commands Command codes F000-FFFF: Vendor unique FC-CT commands.				

Table 104 explains the FC-CT response commands.

Table 104: FC-CT Response Commands

Value	Response
0001-7FFF	Request CT_IU. These codes are used by all CT applications; for an example, see “Name Server Command Codes - Fabric Internal FC-CT Commands” on page 448.
8001	Reject Response CT_IU. These codes are used by all CT applications; for an example, see “FC-CT Reject Reason Code” on page 446.
8002	Accept Response CT_IU (hex ‘0000’: All available information was returned in the Accept CT_IU.)
Other Values	Reserved

Table 105 explains the FC-CT reject reason code.

Table 105: FC-CT Reject Reason Code

Reason	Description
01	Invalid command code
02	Invalid version level
03	Logical error
04	Invalid information unit size
05	Logical busy
07	Protocol error
09	Unable to perform command request
0B	Command not supported
Others	Reserved
FF	Vendor-unique error (see Vendor Unique field)

FC-CT Reason Code Explanation (NS_RJT)

Table 106 provides the Fibre Channel Service Responds (NS_RJT) reason code explanation.

Table 106: FC-CT Reject Reason Code Explanation

Encoded Value (Bits 15-8)	Description
00	No additional explanation
01	Port Identifier not registered
02	Port Name not registered
03	Node Name not registered
04	Class of Service not registered
05	IP Address (node) not registered
06	Initial Process Associator not registered
07	FC-4 TYPEs not registered
08	Symbolic Port Name not registered
09	Symbolic Node Name not registered
0A	Port Type not registered
0B	IP Address (port) not registered
0C	Fabric Port Name not registered
0D	Hard Address not registered
0E	FC-4 Descriptor not registered
0F	FC-4 Features not registered
10	Access denied
11	Unacceptable Port Identifier
12	Data base empty
13	No object registered in the specified scope
Others	Reserved

Table 107 explains the fabric internal FC-CT commands.

Table 107: Name Server Command Codes - Fabric Internal FC-CT Commands

Code	Mnemonic	Description
0410	GE_ID	Get entry, based on port identifier
0420	GE_PN	Get entry, based on port name
0430	GE_NN	Get entries, based on node name
0450	GE_IP	Get entries, based on IP address
04A0	GE_PT	Get entries, based on port type
04B0	GE_ZM	Get entries, based on zone member
04C0	GE_ZN	Get entries, based on zone name
04D0	GE_IPP	Get entries, based on port IP address
04E0	GE_FF	Get entries based on FC-4 features

Table 108 specifies the name server request types.

Table 108: Name Server Request Types

Hexadecimal Code	Description
01*xx*	Get Objects (Query)
02*xx*	Register Object
03*xx*	Deregister Objects
0400-04FF and E000-EFFF	Fabric internal FC-CT commands
F000-FFFF	Vendor unique FC-CT commands

Table 109 describes the name server objects.

Table 109: Name Server Objects

Object Mnemonic	Object Name	Description
A	Aggregated objects	Contains objects 1 through D
ID	Port Identifier	3-byte Address Identifier
PN	Port Name	8-byte Name_Identifier
NN	Node Name	8-byte Name_Identifier
CS	Class of Service	32-bit or 128-bit Internet Protocol address
IPA	Initial Process Associator	8-byte Process_Associator
FT	FC–4 TYPEs	32-byte bit field (8 words), one bit per TYPE supported
SPN	Symbolic Port Name	Variable length (0 to 255-byte) field
SNN	Symbolic Node Name	Variable length (0 to 255-byte) field
PT	Port Type	1-byte encoded Port Type
IPP	IP Address (Port)	32-bit or 128-bit Internet Protocol address
FPN	Fabric Port Name	8-byte Name_Identifier
HA	Hard Address	3-byte Address Identifier
FD	FC-4 Descriptor	Variable length (0 to 255-byte) field
FF	FC-4 Features	128-byte array, four bits per TYPE

Table 110 shows the name server port types.

Table 110: Name Server Port Types

Code	Description
0	NSPT_UNKNOWN
1	N_PORT
2	NL_PORT
3	NFL_PORT
	0x04-0x80 are reserved
0x7F special value for all of the above ports	Nx_PORT
0x81	F_PORT
0x82	FL_PORT
0x83	LT_PORT
0x84	E_PORT

Table 111 explains the name server GS subtype codes.

Table 111: Name Server GS_Subtype Codes

Value	Service
01	Reserved
02	Name Server
03	IP Address Server
80-EF	FC-4 specific Servers
Other values	Reserved

About the FC-4 Type Code

The FC-4 Type Code provides the type of protocol service (for example, FC_CT, FCP, FCIP). Table 112 explains the use of these type codes.

Table 112: FC-4 Type Codes

Code	Service
0x00	Basic Link
0x01	Extend Link
0x04	ISO/IEC 8802-2 LLC/SNAP (in order)
0x05	FCIP
0x08	SCSI_FCP
0x09	SCSI-GPP
0x20	Fibre Channel Services (NS,MS,AS,etc.)
0x21	FC-FG
0x22	FC_SW
0x23	FC-AL
0x24	FC-SNMP
0x25-0x27	Fabric Services
0x30-0x33	Scalable Coherent Interface
0x40	HIPPI-FP
0x58	Virtual Interface
0x5b	Fabric
0xe0 –0xff	Vendor Specific

Table 113 provides the server-to-server command response codes.

Table 113: Server-to-Server Protocol Data Unit Command Response Codes

Code	Description
0x0001	NSS_REQUEST
0x0002	NSS_RESPONSE
0x0003	NSS_INFORM
0x0004	NSS_DELETE

Table 114 shows the NSS_CT command response codes.

Table 114: NSS_CT Command Response Codes

Code	Description
0x0001	NSS_REQUEST
0x0002	NSS_RESPONSE
0x0003	NSS_INFORM
0x0004	NSS_DELETE
0x0410	NSS_GE_ID
0x0420	NSS_GE_PN
0x0430	NSS_GE_NN
0x0450	NSS_GE_IP
0x0470	NSS_GE_FT
0x04A0	NSS_GE_PT

About the Management Server

The Management Service (MS) provides a single management access point within the Fibre Channel Fabric.

The Management Server (MS) Well Known Address = FFFFFA.

Management Service covers the following areas:

- The Fabric Configuration Server provides for the configuration management of the Fabric (see "About the Fabric Configuration Server" on page 453).
- The Unzoned Name Server provides access to Name Server information that is not subject to zone constraints. See "About the Name Server (SNS)" on page 441.
- The Fabric Zone Server provides access to, and control of, zone information (see "About the Fabric Zone Server (ZS)" on page 466).

About the Fabric Configuration Server

The Fabric Configuration Server provides a way for a management applications to discover Fibre Channel Fabric topology and attributes. Requests for the Fabric Configuration Server are carried over the Common Transport. The Fabric Configuration Server is intended to be distributed among Fabric elements, making the Fabric Configuration Server immediately available to an N_Port after it has successfully completed Fabric Login. However, the Fabric Configuration Server is not restricted or required to be part of a Fabric, and may be located in any N_Port or NL_Port.

Fabric Configuration Server Codes

Fabric Configuration Server registration, deregistration and queries are managed through protocols containing a set of Request CT_IUs and Response CT_IUs supported by the Fabric Configuration Server. See Table 104 on page 445.

Management Server Command Codes

Table 115 describes the management server command codes.

Table 115: Management Server Command Codes

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
0x0100	MS_GTIN	Get Topology Information	The Request CT_IU for GTIN contains the request payload defined for the Request Topology Information Extended Link Service.	The Accept CT_IU for GTIN contains the ACC payload defined for the Request Topology Information Extended Link Service.
0x0101	MS_GIEL	Get interconnect element list		List of Interconnect Element Names and Types
0x0111	MS_GIET	Get interconnect element type	Interconnect element name	Interconnect element type
0x0112	MS_GDID	Get domain ID	Interconnect element name	Domain identifier
0x0113	MS_GMID	Get Mgmt Identifier	Interconnect element name	Management Identifier
0x0114	MS_GFN	Get Fabric Name	Interconnect element name	Fabric Name0x0115
0x0115	MS_GLIEN	Get logical IE Name	Interconnect element name	Interconnect element logical name
0x0116	MS_GMAL	Get Mgmt Address list	Interconnect element name	Interconnect element management address list
0x0117	MS_GIEIL	Get IE Information list	Interconnect element name	Interconnect element information list

Table 115: Management Server Command Codes (Continued)

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
0x0118	MS_GPL	Get switch port list	Interconnect element name	List of Port Names, Port Types, Port TX Types, and Port Module Types
0x0121	MS_GPT	Get switch port type	Port Name	Port type
0x0122	MS_GPPN	Get switch physical port number	Port WWN	Port number
0x0124	MS_GAPNL	Get attached port name list	Port WWN	List of attached port name
0x0126	MS_GPS	Get switch port state	Port WWN	Port state (See Port State table)
0x0128	MS_GATIN	Get attached topology information	Port WWN	Attached topology information (4 bytes format)
Get Platform Related Info				
0x0191	MS_GPLNL	Get platform node name list	Platform name	List of platform node name
0x0192	MS_GPLT	Get platform type	Platform name	See Platform type table
0x0194	MS_GPLA	Get platform attributes	Platform name	Platform Mgmt address list
0x01A1	MS_GNPL	Get platform name-node name	Platform Node name	Platform Name
0x01A2	MS_GPNL	Get platform name list	None	List of platform names
0x01B1	MS_GNID	Get node identification data	Platform node name	None. Note that the Accept CT_IU for GNID contains the ACC payload defined for the Request Node Identification Data Extended Link Service.

Table 115: Management Server Command Codes (Continued)

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
0x0215	MS_RIELN	Register IE logic name	Interconnect element Name, Interconnect Element Logical Name	None
Register Platform Related Info				
0x0280	MS_RPL	Register platform	Platform Name, Platform Type, Platform Mgmt Address list, Platform Node Name List	None
0x0291	MS_RPLN	Register platform node name	Platform name, Platform Node Name	None
0x0292	MS_RPLT	Register platform type	Platform Name, Platform Type	None
0x0293	MS_RPLM	Register platform Mgmt address	Platform Name, Platform Mgmt Address	None
De-Register Platform Related Info				
0x0380	MS_DPI	De-register platform	Platform Name	None
0x0391	MS_DPLN	De-register platform node name	Platform Node Name	None
0x0392	MS_DPLM	De-Register Platform Mgmt Addr		None
0x0393	MS_DPLML	De-register platform mgmt address list	Platform Name	None
Port Performance Info				

Table 115: Management Server Command Codes (Continued)

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
0x0400	MS_GPST	Get port statistics		
0x0401	MS_GPERR	Get port errors		
0x0402	MS_PCLST	Clear port stats		
0x0403	MS_PENAB	Port enable		
0x0404	MS_PDISA	Port disable		
Routing Info				
0x0405	MS_GROUT	Get a route between two end ports		
0x0406	MS_GLROUT	Nexthop info from remote switch		
0x0407	MS_GPATH	Output ports to reach a domain		
0x0408	MS_GROUT	Set static route		
0x0750	MS_DELROUT	Delete static route		
Fabric Hierarchy				
0x0501	MS_GFABRIC	Return all switch and port wwns		
0x502	MS_GSW	Return switch and port wwns		
Switch Info				
0x0505	MS_GSWITCH	Get switch information		
0x0506	MS_SSWITCH	Set switch information		
0x0507	MS_GSWITCH2	Get switch information		
0x0508	MS_SSWITCH2	Set switch information 2.0+		
API Version Info				

Table 115: Management Server Command Codes (Continued)

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
0x0509	MS_GAPIVERSION	Get API version		
0x050a	MS_GSSWITCH_NG	Get switch info ng		
0x050b	MS_SSWITCH_NG	Set switch info ng		
0x05010	MS_GPORTLOG	Get port log		
0x05011	MS_GERRLOG	Get error log		
0x05012	MS_GFRULOG	Get FRU history log		
0x05013	MS_GPORTNVLOG	Get port flash log		
Port Info				

Table 115: Management Server Command Codes (Continued)

Code	Mnemonic	Description	Objects in Request CT_IU	Objects in Accept CT_IU
0x0605	MS_GPORT	Get port information		
0x0606	MS_SPORT	Set port information		
0x0607	MS_GPSTATS	Get port stats information		
0x0608	MS_SPSTATS	Set port stats information		
0x0609	MS_GDEVICE	Get device information		
0x060a	MS_GDEVICE2	Get device, string len = 256		
0x060b	MS_GPERRS	Get port err information		
0x060c	MS_SPERRS	Set port err information		
0x060d	MS_GENVATTR	Asset management		
0x060e	MS_GFLPORT	Get fl port info		
0x060f	MS_GMODULE	Get PortModule info		
0x0610	MS_SMODULE	Set PortModule info		
0x0611	MS_GPORT2	Get port info 2		
0x0612	MS_SPORT2	Set port info 2		
0x0613	MS_GPLATINFO	Get platform state info		
0x0614	MS_GPLATALL	Get all platform database		
0x0615	MS_GCP	Get CP info		
0x0616	MS_SFRU	Set FRU Attributes		
0x0617	MS_GENVATTR2	Switch Enclosure Attributes 2		
0x0618	MS_GPORT_NG	Get port info ng		
0x0619	MS_SPORT_NG	Set port info ng		
0x0620	MS_START_PORT_DIAG	Start port diag		

Table 116 shows the management server GS_Subtype codes.

Table 116: GS_Subtype Codes

Code	Server
01	Fabric Configuration Server
02	Unzoned Name Server
03	Fabric Zone Server
04	Reserved for Lock Server
10	FDMI
E0-FF	Vendor Specific Servers
EO	HP Unique MS Subtype. HP API.
E1	MS Telnet subtype. HP Telnet.
E2	HP Unique MS Subtype.
E3	HP API Event.
E4	HP unique subtype. Asynchronous Response Router (ARR).
Other values	Reserved

Management Server Reason Codes and Explanations

If a Fabric Configuration Server request is rejected with a reason code of unable to perform command request, it is because of one of the reason codes shown in Table 117:

Table 117: Management Server Reason Codes and Explanations

Code	Reason
00	No additional explanation
01	Invalid Name_Identifier for Interconnect Element or Port
10	Interconnect Element List not available
11	Interconnect Element Type not available
12	Domain Identifier not available
13	Management Identifier not available
14	Fabric Name not available
15	Interconnect Element Logical Name not available
16	Management Address List not available
17	Interconnect Element Information List not available
	0x18-2F reserved for IE
30	Port List not available
31	Port Type not available
32	Physical Port Number not available
33	Reserved
34	Attached Port Name List not available
35	Reserved
36	Port State not available
50	Unable to register Interconnect Element Logical Name
60	Platform Name does not exist
61	Platform Name already exists
62	Platform Node Name does not exist
63	Platform Node Name already exists.
64	EXPL_PLATFORM_DATABASE_CONFLICT
65	EXPL_PLATFORM_FUNC_UNABLE_TO_ACTIVATE
66	M_E_P_UNABLE_TO_ACTIVATE MSRJT_EXPL_PLATFORM_FUNC_UNABLE_TO_ACTIVATE MSRJT_EXPL_PLATFORM_FUNC_SEC_CONFLICT

Table 117: Management Server Reason Codes and Explanations (Continued)

Code	Reason
67	MSRJT_EXPL_NO_PLATFORM_MGMTADDR
F0	EXPL_AUTHORIZATION_EXCEPTION
F1	EXPL_AUTHEN_EXCEPTION
F2	EXPL_DATABASE_FULL
0x01	MSRJT_EXPL_WWN_INVALID
0x91	MSRJT_EXPL_NO_PORT_STAT
0x92	MSRJT_EXPL_NO_PORT_ERRS
0x93	MSRJT_EXPL_PORT_CLR_FAIL
0x94	MSRJT_EXPL_PORT_ENABLE_FAIL
0x95	MSRJT_EXPL_PORT_DISABLE_FAIL
0x96	MSRJT_EXPL_NO_ROUT_INFO
0x97	MSRJT_EXPL_NO_LOCAL_ROUTE
0x98	MSRJT_EXPL_NO_PATH_INFO
0x99	MSRJT_EXPL_SET_STATIC_ROUTE_FAILED
0xa1	MSRJT_EXPL_DELETE_STATIC_ROUTE_FAILED
0xa5	MSRJT_EXPL_NO_SUCH_SWITCH
Definitions for port info access	
0xb5	MSRJT_EXPL_NO_SUCH_PORT
0xc5	MSRJT_EXPL_INVALID_ARG
0xc6	MSRJT_EXPL_FW_INVALID_CLASS_AREA
0xc7	MSRJT_EXPL_FW_INVALID_INDEX
0xc8	MSRJT_EXPL_FW_INVALID_LEVEL_INDICATOR
0xc9	MSRJT_EXPL_FW_INVALID_EVENT_TYPE
0xca	MSRJT_EXPL_FW_INVALID_ALARM_MATRIX
0xcb	MSRJT_EXPL_FW_INVALID_BUFFER_SIZE
0xcc	MSRJT_EXPL_FW_INVALID_LOW
0xcd	MSRJT_EXPL_FW_INVALID_HIGH
0xce	MSRJT_EXPL_FW_INVALID_TB
0xcf	MSRJT_EXPL_FW_INVALID_UNIT_STRING

Table 117: Management Server Reason Codes and Explanations (Continued)

Code	Reason
0xd0	MSRJT_EXPL_FW_INVALID_STATUS
0xd1	MSRJT_EXPL_FW_INVALID_BT
0xd2	MSRJT_EXPL_FW_INVALID_WWN
0xd3	MSRJT_EXPL_FW_DOWNLOAD_FAILED
0xd4	MSRJT_EXPL_FW_INVALID_PROFILE
0xd5	MSRJT_EXPL_FW_LOAD_FAILED
0xd6	MSRJT_EXPL_FW_INSERT_FAILED
0xd7	MSRJT_EXPL_FW_DOWNLOAD_INIT_FAILED
0xd8	MSRJT_EXPL_FW_TOO_MANY_PROXY
0xd9	MSRJT_EXPL_FW_PROXY_NOT_FOUND
0xda	MSRJT_EXPL_FW_NO_LICENSE
SecureSAN PKI installation support	
0xdb	MSRJT_EXPL_CERT_ALREADY_INSTALLED
0xdc	MSRJT_EXPL_CERT_REQ_FAILED
Firmwaredownload errors	
0xdd	MSRJT_EXPL_CORRUPT_FLASH
	/* attach port stats errors */
0xde	MSRJI_EXPL_RLS_SERVICE_DISABLE
Port cfg errors	
0xe1	MSRJT_EXPL_PORTCFG_FAILED
0xe2	MSRJT_EXPL_PORTCFG_BADPORT
0xe3	MSRJT_EXPL_PORTCFG_BADARG
0xe4	MSRJT_EXPL_PORTCFG_BADNUMARG
0xe5	MSRJT_EXPL_PORTCFG_CFGABT
0xe6	MSRJT_EXPL_PORTCFG_NOLICENSE
0xe7	MSRJT_EXPL_PORTCFG_BADSWTYPE
0xe8	MSRJT_EXPL_PORTCFG_ISQLPORT
0xe9	MSRJT_EXPL_PORTCFG_ISLPORT
0xea	MSRJT_EXPL_PORTCFG_ISGPORT

Table 117: Management Server Reason Codes and Explanations (Continued)

Code	Reason
0xeb	MSRJT_EXPL_PORTCFG_MCASTLB_LBEXIST
0xec	MSRJT_EXPL_PORTCFG_LONGDIST_MCASTON
0xed	MSRJT_EXPL_PORTCFG_LONGDIST_NOLDFAB
0xee	MSRJT_EXPL_PORTCFG_BADPTTYPE
0xef	MSRJT_EXPL_PORTCFG_BADSTRING

Management Server Examples

v4.x

```
portlogdump:
time          task       event    port cmd   args
-------------------------------------------------
15:53:32.201  PORT       Rx        9    164   03fffffd,00fffffd,01a60312,02000000
15:53:32.201  PORT       Tx        9      0   c0fffffd,00fffffd,01a60312
15:53:32.201  PORT       scn       8      1   00000000,00000000,00000002
```

v3.x

Example CT-Management Server - FC-4 Type Device Data

```
22:31:35.366 tReceive   Rx    3   24 02fffc0a,00fffc0b,028dffff,01000000,10cb3a40
22:31:35.366 tTransmit  Tx    3    0 c0fffc0b,00fffc0a,028d025a, ,10cb3a40
22:31:35.366 tTransmit ctin  3   fa 00030124,20000060,69500efa
22:31:35.366 tTransmit ctout 3   fa 00038002,00000001,20080060
22:31:35.366 tSwitch    Tx    3   16 03fffc0b,00fffc0a,028d025a,00000001,10cb44d0
```

Output Line 1:

```
22:31:35.366 tReceive  Rx 3 24 02fffc0a,00fffc0b,028dffff,01000000,10cb3a40
```

Table 118: Breakdown of Argument Fields in Output Line 1

Argument 1 02fffc0a	Argument 2 00fffc0b	Argument 3 028dffff	Argument 4 01000000	Argument 5 10cb3a40
02 = RC_CTL (request)	00 = Identifier	028d = OX_ID	01000000 = FC-CT IU Preamble; "01" = CT revision	10cb3a40 = IU address pointer
fffc0a = D_ID	fffc0b = S_ID	ffff = RX_ID		

Output Line 2:

```
22:31:35.366 tTransmit Tx 3 0 c0fffc0b,00fffc0a,028d025a, ,10cb3a40
```

Table 119: Breakdown of Argument Fields in Output Line 2

Argument 1 c0fffc0b	Argument 2 00fffc0a	Argument 3 028d025a	Arg 4	Argument 5 10cb3a40
c0 = RC_CTL(Link Control acknowledge)	00 = Identifier	028d = OX_ID	Null	10cb3a40 = IU address pointer
fffc0b = D_ID	fffc0a = S_ID	025a = RX_ID		

Output Line 3:

```
22:31:35.366 tTransmit ctin 3 fa 00030124,20000060,69500efa
```

— `0124` = CT-Management Server Code. Get a list of port names for this port WWN "200000606950efa".

Output Line 4:

```
22:31:35.366 tTransmit ctout 3 fa 00038002,00000001,20080060
```

— 8002 = CT-Management Server code. "8002" = accept.

Output Line 5:

```
22:31:35.366 tSwitch Tx 3 16 03fffc0b,00fffc0a,028d025a,00000001,10cb44d0
```

Table 120: Breakdown of Argument Fields in Output Line 5

Argument 1 03fffc0b	Argument 2 00fffc0a	Argument 3 028d025a	Argument 4 00000001	Argument 5 10cb44d0
03 = RC_CTL (reply)	00 = Identifier	028d = OX_ID	00000001 = response object	10cb44d0 = IU address pointer
fffc0b = D_ID	00fffc0a = S_ID	025a = RX_ID		

Example Summary:

Embedded switch `fffc0a` requests from the embedded switch `fffc0b` a list of port names for the device with WWN `200000606950efa`. The response from `fffc0b` is accepted.

About the Fabric Zone Server (ZS)

The Fabric Zone Server adds and removes activations. Queries are managed through protocols containing a set of Request CT_IUs and Response CT_IUs supported by the Fabric Zone Server. For a Fabric Zone Server request, the payload is transported from the requestor to the Fabric Zone Server using a Request CT_IU. The corresponding Fabric Zone Server response is transported from the Fabric Zone Server to the requestor, in the Exchange established by the requestor, using a Response CT_IU.

The request codes described Table 121 are based on Section 6.3 (Fabric Zone Server) of FC-GS4 rev 7.1 dtd Sep 19, 2001. HP supports only those codes that are compatible with zoning.

Fabric Zone Server (ZS) Codes

Table 121 explains the fabric zone server request command codes.

Table 121: Fabric Zone Server Request Command Codes

Code (hex)	Mnemonic & Description	Attributes in Request CT_IU	Attributes in Accept CT_IU
0100	GZC Get Capabilities	None	Capabilities
0111	GEST Get Enforcement State	None	Enforcement state
0112	GZSN Get Zone Set List	None	List of Zone Set Name and Number of Zones
0113	GZD Get Zone List	Zone Set Name	List of Zone Names and Number of Zone Members
0114	GZM Get Zone Member List	Zone Name	List of Zone Member Identifier Types and ZoneMember Identifiers
0115	GAZS Get Active Zone Set	None	Zone Set Name; Number of Zones; List of Zone Names, Number of Zone Members, List of Zone Member Identifier Types and Zone Member Identifiers
0116	GZS Get Zone Set	Zone Set Name	None
0200	ADZS Add Zone Set	Zone Set Name; Number of Zones; List of Zone Names, Number of Zone Members, List of Zone Member Identifier Types and ZoneMember Identifiers	None
0201	AZSD Activate Zone Set Direct	Zone Set Name; Number of Zones; List of Zone Names, Number of Zone Members, List of Zone MemberIdentifier Types and ZoneMember Identifiers	None
0202	AZS Activate Zone Set	Zone Set Name	None

Table 121: Fabric Zone Server Request Command Codes (Continued)

Code (hex)	Mnemonic & Description	Attributes in Request CT_IU	Attributes in Accept CT_IU
0203	DZS Deactivate Zone Set	None	None
0204	AZM Add Zone Members	Zone Name; List of Zone MemberIdentifier Types and ZoneMember Identifiers	None
0205	AZD Add Zone	Zone Set Name; Zone Name	None
0300	RZM Remove Zone Members	Zone Name; List of Zone MemberIdentifier Types and ZoneMember Identifiers	None
0301	RZD Remove Zone	Zone Set Name; Zone Name	None
0302	RZS Remove Zone Set	Zone Set Name	None
0x0120	ZS_GZA	Get Zone Attributes	
0x0122	ZS_GZSE	GET ZONE SET list-Enhanced	
0x0123	ZS_GZDE	Get zone list-Enhanced	

Table 121: Fabric Zone Server Request Command Codes (Continued)

Code (hex)	Mnemonic & Description	Attributes in Request CT_IU	Attributes in Accept CT_IU
0x0124	ZS_GZME	Get Zone Member List-Enhanced	
0x0126	ZS_GZSE	Get Zone Set - Enhanced	
0x0128	ZS_GAL	Get Alias List	
0x0129	ZS_GAM	Get Alias Member List	
0x0210	ZS_AZSE	Add Zone Set - Enhanced	
0x0220	ZS_CZS	Create Zone Set	
0x0224	ZS_AZME	Add Zone Members-Enhance d	
0x0225	ZS_CZ	Create Zone - Enh v. 0.31	
0x0228	ZS_SZA	Set Zone Attributes	
0x0229	ZS_CA	Create Alias - Enh v. 0.31	
0x0229	ZS_AA	Add Alias	
0x022A	ZS_AAM	Add Alias Members	
0x0321	ZS_RZ	Remove Zones	
0x0324	ZS_RZME	Remove Zone Members-Enhance d	
0x0329	ZS_RA	Remove Alias	
0x032A	ZS_RAM	Remove Alias Members	

Table 122 explains the zone server reject CT_IU reason codes.

Table 122: Zone Server Reject CT_IU Reason Codes Explanations

Hexadecimal Code	Description
	GS4-codes
0x00	ZS_RJT_EXPL_NONE
0x01	ZS_RJT_EXPL_ZONES_NOT_SUPPORTED
0x10	ZS_RJT_EXPL_ZONESET_NAME_UNKNOWN
0x11	ZS_RJT_EXPL_NO_ZONESET_ACTIVE
0x12	ZS_RJT_EXPL_ZONE_NAME_UNKNOWN
0x13	ZS_RJT_EXPL_ZONE_STATE_UNKNOWN
0x14	ZS_RJT_EXPL_INCORRECT_PAYLOAD_LENGTH
0x15	ZS_RJT_EXPL_ZONESET_TOO_LARGE
0x16	ZS_RJT_EXPL_DEACTIVATE_FAILED
0x17	ZS_RJT_EXPL_REQUEST_NOT_SUPPORTED
0x18	ZS_RJT_EXPL_CAPABILITY_NOT_SUPPORTED
0x19	ZS_RJT_EXPL_MEMBER_TYPE_NOT_SUPPORTED
0x1A	ZS_RJT_EXPL_INVALID_ZONESET
	Enhanced *GS-4* codes
0x20	ZS_RJT_EXPL_ENHANCED_CMDS_NOT_SUPPORTED
0x21	ZS_RJT_EXPL_ZONE_SET_ALREADY_EXISTS
0x22	ZS_RJT_EXPL_ZONE_ALREADY_EXISTS
0x23	ZS_RJT_EXPL_ALIAS_ALREADY_EXISTS
0x24	ZS_RJT_EXPL_ZONE_SET_UNKNOWN
0x25	ZS_RJT_EXPL_ZONE_UNKNOWN
0x26	ZS_RJT_EXPL_ALIAS_UNKNOWN
0x28	ZS_RJT_EXPL_NAME_UNKNOWN
0x29	ZS_RJT_EXPL_NAME_ALREADY_EXISTS
0x30	ZS_RJT_EXPL_COMMIT_FAILED

Alias Service

Table 123 specifies the alias service request codes.

Table 123: Alias Service Request Codes (FC_GS-1)

Code	Abbreviation	Description
0	ASRV_OK	Alias service OK.
0	ASRV_ACC	Alias service accepted.
1	ASRV_REJ	Alias service. See FS_RJT reason code explanation.
2	ASRV_NOBUF	Alias service - no buffer.
3	ASRV_INVALID	Alias service - invalid parameter.
4	ASRV_BADPTR	Alias service - bad pointer.
11	ASRV_DB_ENTRY_EXIST	Related to database.
12	ASRV_DB_NOENTRY	Alias service - no entry.
19	ASRV_DB_CORRUPTED	Alias service - this is a critical message.

The ctin and ctout Event Examples

v4.x

```
portlogdump:
time          task       event  port cmd  args
-------------------------------------------------
15:53:40.971  nsd        ctin     9   fc  000104a0,0000007f
15:53:40.971  nsd        ctout    9   fc  00018001,00050000
15:53:40.973  PORT       Tx       9   16  03fffca0,00fffc01,033301c7,01000000
15:53:40.980  PORT       Rx       9    0  c0fffc01,00fffca0,033301c7
```

— fc = Name Server in Management Server entries.

v3.x

```
12:06:16.433  tReceive  Rx3  0  20   02  fffffc,00011000,a838ffff,01000000 1st frame
12:06:16.433  tNSd      ctin    0    fc  00010173,00000008
12:06:16.433  tNSd      ctout   0    fc  00018001,00090700   2nd frame
12:06:16.433  tNSd      Tx3     0     0  03011000,00fffffc,a838000e
```

Decoding a ctin Event

Example of MS > Name Server

```
12:06:16.433   tNSd        ctin      0    fc   00010173,00000008
```

1. Note the `fc` in the `cmd` field. FC = Name Server for MS entries.
2. Divide argument 1 into two 16-bit fields: 0001 and 0173
   - The first 16-bit field is the bit map, which indicates whether subsequent arguments are valid.
     - — A `0001` entry (1 = 0001 in binary) means the that only one additional argument follows after argument 1 (in this example, 00000008). See CT_IU Frame below.
     - — If the first 16-bit field is `0003`, the arguments in position 1 and 2 are sets, thus you should have two arguments. In other words, two arguments follow argument 1.
   - The second 16-bit field `0173` is the FC_CT command code. `0173` means GNN_FT - Get FC-4 Node Name. See CT_IU Frame below. And the FC-4 object is defined by argument 2 as `00000008`. Argument 2 belongs to word 4 of the GNN_FT frame. See Table 124. Note that `08` means SCSI-FCP.

Table 124: Get FC4-Type Node Name, 0173 Frame

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	FC_CT Rev=01	IN_ID (S to zero by the Requesting_CT)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Command Code = 0173		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Reserved	Domain ID scope	Area_ID scope	FC-4 Type Code=08

Decoding a ctout Event

Example

```
12:06:16.433  tNSd      ctout    0   fc  00018001,00090700
```

1. Note the `fc` in the `cmd` field. FC = Name Server for MS entries.
2. Take argument 1 and divide into two 16-bit fields: 0001 and 8001
   a. The first 16-bit field `0001` is the bit map, indicating whether subsequent arguments are valid.
      — A `0001` entry (1 = 0001 in binary) means the that only one additional argument follows argument 1 (in this example, 00000008).
      — If the first 16-bit field is `0003`, the arguments in position 1 and 2 are sets, thus you should have two arguments. In other words, two arguments follow argument 1.
   b. The second 16-bit field represents the FC_CT response code.
      — If the second 16-bit field is a reject (`8001`) - then argument 2 is a reject, see Table 105 on page 446. (The example below is 00090700).
      — If the second 16-bit field is an accept (`8002`), then arguments 2 and 3 are the IU response objects.

Table 125 shows the accept get FC4-type node names.

Table 125: Accept Get FC4-Type Node Names, 0173 Frame

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Command Code = 8001		Maximum/Residual Size	
3	Reserved	Reason Code =09	Reason Code Explanation = 07	Vendor Unique
4	Control	Port Identifier#1		
5	Reserved			
6 - 7	Node Name #1			

Link Control Frames

About Link Control Frames

Link Control frames are used to indicate successful or unsuccessful delivery of data frames, to control the flow of data frames, and to provide some low-level N_port commands.

Link Control Headers

ACK Frame

ACK_1, one data frame in a sequence
(RCTL = C0)

ACK Frame					
	Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
H	0	C0	D_ID		
E	1	CS_CTL	S_ID		
A	2	Type =00	F_CTL		
D	3	SEQ_ID	DF_CTL=00	SEQ_DNT	
E	4	OX_ID		RX_ID	
R	5	0000(Reserved)	History bit (see note)	Number of frames being acknowledge	

Note: When bit 16 (history bit) is set to 0, it indicates all previous ACKs of that sequence have been sent.When bit 16 (history bit) is set to 1, it indicates at least one previous ACK has not been sent.

F_BSY Frame

Fabric Busy (F_BSY) Frame
(RCTL = C5 or C6)

Fabric Busy (F_BSY) Frame					
	Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
H	0	C5 or C6	D_ID		
E	1	CS_CTL	S_ID		
A	2	Reason Code	F_CTL		
D	3	SEQ_ID	DF_CTL	SEQ_DNT	
E	4	OX_ID		RX_ID	
R	5	Parameter fields			

F_RJT and N_RJT Frames

See "Fabric Services Reject Reason Codes" on page 433 for reject reason information.

	Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
H	0	C5 or C6	D_ID		
E	1	CS_CTL	S_ID		
A	2	Type	F_CTL		
D	3	SEQ_ID	DF_CTL	SEQ_DNT	
E R	4	OX_ID		RX_ID	

When Action Code is set to 0x01, it indicates the sequence is terminated. When it is set to 0x02, it means the sequence is still alive.

Link Control Frames

P_BSY UI Frame

(RCTL = C4)

	Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
H	0	C4	D_ID		
E	1	CS_CTL	S_ID		
A	2	Type	F_CTL		
D	3	SEQ_ID	DF_CTL	SEQ_DNT	
E	4	OX_ID		RX_ID	
R	5	Action Code	Reason Code	0x00 (Reserved)	Vendor
When Action Code is set to 0x01 it indicates the sequence terminated. When it set to 0x02 if means the sequence is still alive.					

When Action Code is set to 0x01, it indicates the sequence is terminated. When it set to 0x02, it means the sequence is still alive.

No Operation Frame (NOP)

	Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
H	0	80	D_ID		
E	1	CS_CTL=00	S_ID		
A	2	Type =00	F_CTL		
D	3	SEQ_ID	DF_CTL=00	SEQ_DNT	
E	4	OX_ID		RX_ID	
R	5	Parameter			

Abort Sequence Frame (ABTS)

	Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
H	0	81	D_ID		
E	1	CS_CTL=00	S_ID		
A	2	Type =00	F_CTL		
D	3	SEQ_ID	DF_CTL=00	SEQ_DNT	
E	4	OX_ID		RX_ID	
R	5	Parameter			

Basic Accept Frame for ABTS

	Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
H	0	84	D_ID		
E	1	CS_CTL=00	S_ID		
A	2	Type =00	F_CTL		
D	3	SEQ_ID	DF_CTL=00	SEQ_DNT	
E	4	OX_ID		RX_ID	
R	5	Parameter			
	6	Set_ID valid (80=valid, 00=not)	Last SEQ_ID	Reserved	
	7	OX_ID Aborted		RX_ID Aborted	
	8	Low SEQ_CNT		High SEQ_CNT)	

Basic Reject Frame for ABTS

	Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
H	0	85	D_ID		
E	1	CS_CTL=00	S_ID		
A	2	Type =00	F_CTL		
D	3	SEQ_ID	DF_CTL=00	SEQ_DNT	
E	4	OX_ID		RX_ID	
R	5	Parameter			
	6	Reserved	Reason	Explanation	Vendor

Link Control Codes

Table 126 shows the F_BSY reason codes. For Frame information, see “F_BSY Frame” on page 475.

Table 126: F_BSY Reason codes

R_CTL	Code	Meaning
C5	1x	The Fabric is busy
	3x	The destination N_Port is busy with a Class-1 connection
C6	10	The Fabric is busy; ACK_1 is not retransmitted
	11	The Fabric is busy; ACK_N or ACK_0 is not retransmitted
	12	The Fabric is busy; N_Port is rejecting.
	13	The Fabric is busy; Fabric is rejecting.
	17	The Fabric is busy; Link Credit Reset.
	18	The Fabric is busy; Notify.
	19	The Fabric is busy; End.
	30	ACK_1 is not retransmitted.
	31	ACK_0 or ACK_N is not retransmitted.
	32	N_Port is rejecting; the destination N_Port is engaged in a Class-1 connection.
	33	Fabric is rejecting; the destination N_Port is engaged in a Class-1 connection.
	37	Link Credit Reset; the destination N_Port is engaged in a Class-1 connection.
	38	Notify; the destination N_Port is engaged in a Class-1 connection.
	39	End; the destination N_Port is engaged in a Class-1 connection.
	Others	Reserved

P_BSY Action and Reason Codes

P_BSY Action and Reason Codes		
Action code	**Reason Code**	**Meanings**
01 or 02	01	Physical N_Port is busy
	03	A required resource is busy
	07	Partial Multicast busy
	FF	Vendor Unique is busy

F_RJT and N_RJT Action and Reason Codes

See "F_RJT and N_RJT Frames" on page 475 for Frame information.

F_RJT and N_RJT Action and Reason Codes		
Action code	**Reason Code**	**Meanings**
01	01	Invalid D_ID
	02	Invalid S_ID
	03	N_Port temporarily not available
	04	N_Port permanently not available
	05	Class of service not supported
	16	Login required
	17	Excessive sequences attempted
	18	Unable to establish exchange
	19	Reserved
02	09	Invalid R_CTL
	0A	Invalid F_CTL
	0B	Invalid OX_ID
	0C	Invalid RX_ID
	0D	Invalid SEQ_ID
	0E	Invalid DF_CTL
	0F	Invalid SEQ_CNT
	10	Invalid Parameter field
	11	Exchange error
	12	Protocol error
	13	Incorrect length
	14	Unexpected ACK
	15	Class of service not supported by the entity at FFFFFE
	1A	Fabric path not available
	1B	Invalid VC_ID
	1C	Invalid CS_CTL
	1D	Insufficient Resources
	1E	Dedicated Simplex not supported
	1F	Invalid class of services
	20	Preemption request rejected
	21	Preemption not enabled
	22	Multicast error
	23	Multicast error terminate
	FF	Vendor unique
	Others	Reserved

Link Control Abort Sequence (ABTS)

Reject Reason for ABTS

Basic Reject Reason for ABTS	
Reason Code	**Meanings**
01	Invalid (R_CTL) command code
03	Logical error; service requested was invalid or inconsistent.
05	Logical Busy; unable to process service
07	Protocol Error; other FC-2 error
09	Unable to perform a request
Ff	Vendor Unique error

Reject Reason Explanation for ABTS

Basic Reject Reason Explanation for ABTS	
Reason Code	**Meanings**
00	Invalid (R_CTL) command code
03	Logical error; service requested was invalid or inconsistent.
05	Logical Busy; unable to process service
Other value	Reserved

Payload Information

This section describes the following types of Payload Frames:

- "SW_ELS Payload Frames" on page 481
- "SW_ILS Payload Frames" on page 485
- "FC-CT Payload Frames" on page 493

SW_ELS Payload Frames

See "Extended Link Service (ELS)" on page 399 for command information.

ELS Acceptance Frame

ELS Acceptance				
Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	ELS command =02	000000		
n	ELS specific parameters (if present)			

ELS Rejection Frame

ELS Rejection				
Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	ELS Command =01	000000		
1	Reserved	Reason Code	Reason Explanation	Vendor Unique

N_Port Logout Frame

N_Port Logout (LOGO)				
Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	Command =x'05'	X'00'	X'00'	X'00'
1	Reserved	N_Port Identifier		
2-3	Port_Name of the LOGO originator			

PDISC, FDISC,FLOGI, PLOGI

Port Discover (PDISC) 'x50', Fabric Discover (FDISC) x'51', FLOGI = x'04', N_Port login (PLOGI) x'03'				
Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	Command =x'03,04,50,51'	X'00'	X'00'	X'00'
1-4	Common Service Parameters			
5-6	N_Port Name			
7-8	Node Name			
9-12	Class-1 Service Parameters			
13-17	Class-2 Service Parameters			
18-21	Class-3 Service Parameters			
22-25	Class-4 Service Parameters			
26-29	Vendor Version Level			
30-31	Service Availability			
	Reserved			
Note - The Fabric Discover link service (FDISC) allows an N_Port to exchange service parameters with the Fabric without affecting the operating parameters between the N_Port and the Fabric.				

ADISC Frame

Discover Address (ADISC)				
Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	Command =x'52'	X'00'	X'00'	X'00'
1	Reserved	Hard address of originator		
2-3	Port_Name of originator			
4-5	Node_name of originator			
6	Reserved	N_Port ID of originator		

PRLI and PRLO Frames

PRLI and Process Logout (PRLO),x'21'				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command =x'20', x'21'	Page length=x'10'	Payload length	
1-n	Service Parameter Page			

SCN Frame

State Change Notification (SCN)				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	ELS Command =x'60'	Page Length=x'04'	Payload length	
1-n	Affected N_Port ID Pages			
Page Length: The length in bytes of an Affected N_Port ID page. This value is fixed at hex '04'. **Payload Length:** The length in bytes of the entire payload, inclusive of the word 0. This value shall be a multiple of 4. The minimum value of this field is 4. The maximum value of this field is 256. **Affected N_Port ID page:** Each Affected N_Port ID page contains the ID of an Affected N_Port or NL_Port. The RSCN payload may contain zero or more of these pages.				

SCR Frame

State Change Registration (SCR)				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	ELS Command =x'62'	X'00'	X'00'	X'00'
1	Reserved			Registration Function
Function Value 0 = Reserved 1 (Fabric Detected registration) - Register to receive all RSCN requests issued by the Fabric Controller for events detected by the fabric. 2 (N_Port Detected registration) - Register to receive all RSCN requests issued by the Fabric Controller for events detected by the Affected N_Port or NL_Port. 3 (Full registration) - Register to receive all RSCN requests issued by the Fabric Controller. The RSCN request shall return all Affected N_Port ID pages. 4 = Reserved 4 – 254 (Clear registration) - Remove any current RSCN registrations. 255				

RSCN Frame

Registration State Change Notification				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	ELS Command =x'61'	Page Length	Payload Length	
n	Affected N_Port ID Pages (4 bytes each)			
Page Length: The length in bytes of an Affected N_Port ID page. This value is fixed at hex '04'. **Payload Length:** The length in bytes of the entire payload, inclusive of the word 0. This value shall be a multiple of 4. The minimum value of this field is 4. The maximum value of this field is 256. **Affected N_Port ID page:** Each Affected N_Port ID page contains the ID of an Affected N_Port or NL_Port. The RSCN payload may contain zero or more of these pages.				

LISM Frame

LISM Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command code = 11010000			
1-2	Port_Name			

LIFA, LIPA, LIHA and LISA Frames

Payload format for LIFA, LIPA, LIHA and LISA Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command code = 110[2-5]0000			
1	L	Bit Map of AL_PAs		
2-4	Bit Map of AL_PAs (continued)			

FAN Frame

FAN Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command =x'60000000'			
1	L	Loop Fabric Address		
2-3	Fabric Port_Name			
4-5	Fabric_Name			
Fabric Address Notification (FAN) is sent by the FL_Port using an S_ID of x'FFFFFE' to each NL_Port currently logged in to that FL_Port. The purpose of FAN was to allow the FL_Port to provide information to all logged-in NL_Ports on an arbitrated loop following loop initialization.				

LIRP and LILP Frames

LIRP and LILP Frames				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Loop Initialization Code (0x11060000-0x11070000)			
1	Count (Total AL_PA count in list)	1st AL_PA (Master's ALPA)	2nd AL_PA	• • • continue-list AL_PAs
2-26	List of AL_PA (**Note -** FF means AL_PA is not present.)			

SW_ILS Payload Frames

See "Switch Fabric Internal Link Services (SW_ILS)" on page 409 for command information.

SW_ILS Acceptance Frame

ELS Acceptance				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	ELS command =02	000000		
n	ELS specific parameters (if present)			

SW_ILS Reject Frame

See "SW_ILS Reject Reason Codes (SW_RJT)" on page 411 for reject information. See "SW_ILS Reject Example" on page 418 to view an example.

SW_RJT				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	SW_ILS Command Codes =01000000			
1	Reserved	Reason Code	Explanation	Vendor Unique

SW_ILS ELP Request Frame

ELP Request				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	SW_ILS Command Codes =10xxxxxx			
1	Revision	Flags		Reserved
2	R_A_TOV			
3	E_D_TOV			
4-5	Requester Interconnect Port Name			
6-7	Requester Switch Name			
8-9	Class F Service Parameters 16			
10	Class 1 Interconnect Port Parameters			
11	Class 2 Interconnect Port Parameters			
12	Class 3 Interconnect Port Parameters			
13-17	Reserved			
18	ISL Flow Control Mode		Flow Control Parameter Length (N)	
N	Flow Control Parameters			

SW_ILS ELP Accept Frame

ELP Accept				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
6	SW_ILS Command Codes =02000000			
7	Revision =02	Reserved		
8	R_A_TOV			
9	E_D_TOV			
10-11	Responder Interconnect Port Name			
12-13	Responder Switch Name			
14-17	Class F Service Parameters 16			
18	Class 1 Interconnect Port Parameters			
19	Class 2 Interconnect Port Parameters			
20	Class 3 Interconnect Port Parameters			
20-24	Reserved			
25	ISL Flow Control Mode		Flow Control Parameter Length (N)	
N	Flow Control Parameters			

SW_ILS EFP Request Frame

EFP Request Payload				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command code =11	Record length =10	Payload length	
1	Reserved			Principal switch priority
2-3	Principal Switch Name			
4-7	Domain ID List (see SW_ISL – Domain ID list format)			
N	Multicast ID List			

Domain ID List Format

Item	Size (Bytes)
Record_Type	1 byte 00 = reserved 01 =Domain ID List record 02 = Multicast ID List record all other = reserved
Domain_ID	1
Reserved	2
Reserved	4
Switch_Name for Domain_ID	8

Multicast ID List Format

Item	Size Bytes
Record_Type	1 byte 1 byte 00 = reserved 01 =Domain ID List record 02 = Multicast ID List record all other = reserved
Multicast_Group_number	1
Reserved	2
Reserved	12

DIA Request Frame

DIA Request				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command code = 12000000			
1-2	Originating Switch Name			
3	Not Meaningful			

DIA Accept Frame

DIA Accept				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command code = 02000000			
1-2	Responding Switch Name			
3	Not Meaningful			

RDI Request Frame

RDI Request				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command code = 13	Reserved	Payload Length	
1-2	Requesting Switch Name			
3	Reserved			Requested Domain ID#1
4	Reserved			Requested Domain ID#2
n	Reserved			Requested Domain ID#n

RDI Accept Frame

RDI Accept				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command code = 02	Reserved	Payload Length	
1-2	Requesting Switch Name			
3	Reserved			Granted Domain ID#1
4	Reserved			Granted Domain ID#2
n	Reserved			Granted Domain ID#n

BF (Build Fabric) Frame

BF Request				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	17	00	00	00
For use in Fabric Configuration, the S_ID field shall be set to hex’FFFFFD’, indicating the Fabric Controller of the originating Switch. The D_ID field shall be set to hex’FFFFFD’, indicating the Fabric Controller of the destination Switch.				

RCF Frame

RCF Request				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	18	00	00	00
For use in Fabric configuration, the S_ID field shall be set to hex’FFFFFD’, indicating the Fabric controller of the originating switch. The D_ID field shall be set to hex’FFFFFD’, indicating the Fabric controller of the destination switch.				

FSPF Header Format

FSPF header Format				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	Command code			
1	FSPF version	AR Number	Authentication Type	Reserved
2	Originating Domain ID			
3-4	Authentication			

HLO Request Frame

FSPF HLO Request Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
FSPF Header (word 0-4)	Command code =14000000			
	FSPF version =02	AR Number =00	Authentication Type =00	Reserved
	Originating Domain ID			
	Authentication =00000000			
5	Reserved (option)			
6	Hello Interval			
7	Dead Interval			
8	Reserved	Originating Port Index		

LSU Request Frame

Link Status Updated Request Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
FSPF Header (word 0-3)	Command code =13000000			
	FSPF version =02	AR Number =00	Authentication Type =00	Reserved
	Originating Domain ID			
	Authentication =00000000			
5	Reserved			Flags
6	Number of Link State Records			
n	Link State Records			

Flags Field Bit Map

Bit	Description
0	Data Base Exchange – Value b'1' - LSU is used for initial database synchronization Value b'0' - LSU is used for a topology update
1	Database Complete Value b'1' - Last sequence of data base synchronization. LSU contains no LSRs. Value b'0' - Not the last sequence of database synchronization
2-7	Reserved

Link State Record Header Format

Link State Record Header				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	LSR Type	Reserved	LSR Age	
1	Reserved			
2	Link State Identifier			
3	Advertising Domain ID			
4	Link State Incarnation Number			
5	Check Sum		LSR Length	

Link State Descriptor

<table>
<tr><th colspan="5">Link State Descriptor</th></tr>
<tr><th>Word</th><th>Bits 31-24</th><th>Bits 23-16</th><th>Bits 15-8</th><th>Bits 7-0</th></tr>
<tr><td rowspan="4">FSPF Header (Word 0-3)</td><td colspan="4">Command code =15000000</td></tr>
<tr><td>FSPF version =02</td><td>AR Number =00</td><td>Authentication Type =00</td><td>Reserved</td></tr>
<tr><td colspan="4">Originating Domain ID</td></tr>
<tr><td colspan="4">Authentication =00000000</td></tr>
<tr><td rowspan="6">Link State Recorder Header (Word 4-9)</td><td>LSR Type =01</td><td>Reserved</td><td colspan="2">LSR Age</td></tr>
<tr><td colspan="4">Reserved</td></tr>
<tr><td colspan="4">Link State Identifier</td></tr>
<tr><td colspan="4">Advertising Domain ID</td></tr>
<tr><td colspan="4">Link State Incarnation Number</td></tr>
<tr><td colspan="2">Check sum</td><td colspan="2">LSR Length</td></tr>
<tr><td>10</td><td colspan="2">Reserved</td><td colspan="2">Number of Links</td></tr>
<tr><td>11-14</td><td colspan="4">Link Descriptor #1</td></tr>
<tr><td>15-18</td><td colspan="4">Link Descriptor #2</td></tr>
<tr><td>n</td><td colspan="4">Link Descriptor # n</td></tr>
</table>

LSA Request Frame

<table>
<tr><th colspan="5">Link State Acknowledged Request</th></tr>
<tr><th>Word</th><th>Bits 31-24</th><th>Bits 23-16</th><th>Bits 15-8</th><th>Bits 7-0</th></tr>
<tr><td rowspan="4">FSPF Header (Word 0-4)</td><td colspan="4">Command code =16000000</td></tr>
<tr><td>FSPF version =2</td><td>AR Number =00</td><td>Authentication Type =00</td><td>Reserved</td></tr>
<tr><td colspan="4">Originating Domain ID</td></tr>
<tr><td colspan="4">Authentication</td></tr>
<tr><td>5</td><td colspan="3">Reserved</td><td>Flags</td></tr>
<tr><td>6</td><td colspan="4">Number of Link State Record Headers</td></tr>
<tr><td rowspan="6">Link State Header</td><td>LSR Type</td><td>Reserved</td><td colspan="2">LSR Age</td></tr>
<tr><td colspan="4">Reserved</td></tr>
<tr><td colspan="4">Link State Identifier</td></tr>
<tr><td colspan="4">Advertising Domain ID</td></tr>
<tr><td colspan="4">Link State Incarnation Number</td></tr>
<tr><td colspan="2">Check Sum</td><td colspan="2">LSR Length</td></tr>
</table>

FC-CT Payload Frames

See "FC-CT Frame" on page 438 for Frame-related information.

FC-CT Payload Diagram

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
H	R_CTL =02 or 03	D_ID		
E	CS_CTL=00	S_ID		
A	Type =20	F_CTL		
D	SEQ_ID	DF_CTL	SEQ_DNT	
E	OX_ID		RX_ID	
R	Parameter			
6	FC-CT Header Usage			

FC-CT Header Usage

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0-3	Basic CT_IU preamble			
4-25	Extended CT_IU preamble			

Note: This reference covers only the Basic CT-IU Preamble.

Basic CT_IU Preamble

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique

CT-IU Request

GA_NXT (0100), GPN_ID (0112), GNN_ID (0113),GCS_ID (0114), GFT_ID (0117), GSPN_ID (0118), GPT_ID (011A), GIPP_ID (011B), GFPN_ID (11C), GHA_ID (011D), GFF_ID (011F)

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Reserved	Port Identifier		

Get Identifier - GID-A (0101)

Get Identifier {GID-A (0101) }				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Reserved	Domain_ID scope	Reserved	

GFD_ID (011E)

Get FC-4 Descriptors, 011E Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Reserved	Port Identifier		
5-12	FC-4 Types (32 bytes)			

Get IP Address - GIPP_PN (012B)

Get IP Address (Port), 012B Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Port Name			

GID_NN (0131)

Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Node Name			

Get FC4- Type Node Name - GNN_FT (0173)

Get FC4-Type Node Name, 0173 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Reserved	Domain ID scope	Area_ID scope	FC-4 Type Code

GID_PT (01A1)

Get Port Identifiers, 01A1 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Port Type	Domain ID scope	Area_ID scope	Reserved

CT_IU Response

GA_NXT (0100)

Accept – All CT-IU request, 0100 Frame	
Item	**Size (Bytes)**
CT_IU preamble	16
Port Type	1
Port Identifier	3
Port Name	8
Length of Symbolic Port Name (m)	1
Symbolic Port Name	m
Reserved	255-m
Node Name	8
Length of Symbolic Node Name (n)	1
Symbolic Node Name	n
Reserved	255-n
Initial Process Associator	8
IP Address (Node)	16
Class of Service	4
FC–4 TYPEs	32
IP Address (Port)	16
Fabric Port Name	8
Reserved	1
Hard Address	3

GID_A (0101)

Accept Domain_ID Scope is zero, 0101 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Control	Domain ID#1	Reserved	
5	Control	Domain ID#2	Reserved	
n	Control	Domain ID#n	Reserved	

Accept Domain_ID Scope is non-zero, 0101 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Control	Request Domain ID#1	Reserved	
5	Control	Request Domain ID#2	Reserved	
n	Control	Request Domain D#n	Reserved	

GPN_ID (0112)

Accept Port Name, 0110 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Port Name			

GNN-ID (0113)

Accept Node Name, 0113 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Node Name			

GCS-ID (0114)

Accept Class of Service, 0114 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Class of Service			

GFT-ID (0117)

Accept FC-4 Type, 0117 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4-11	FC4-type (32 bytes)			

GSPN_ID (0118)

Accept Symbolic Port Name, 0118 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
m	Name Length (m)	Symbolic Port Name		
n	Reserved (255 bytes +m)			

GPT_ID (011A)

Accept Port Type, 011A Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Port Type	Reserved		

GIPP_ID (011A)

Accept IP Address (Port), 011B Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4-7	IP Address Port			

GFPN_ID (011C)

Accept Fabric Port Name, 011C Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4-5	Fabric Port Name			

GHA_ID (011D)

Accept Hard Address, 011D Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Reserved	Hard Address		

GNN_FD (0173)

Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Command Code =0173		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Control	Port Identifier#1		
5	Reserved			
6-7	Node Name #1			

GFD_ID (011E)

Accept FC-4 Descriptor, 011E FRame	
Item	Size(Bytes)
CT_IU preamble	16 (see p.85)
Descriptor length (m) #1	1
FC-4 Descriptor #1	m
Reserved	255-m
. . .	.....
Descriptor length (m) #n	1
FC-4 Descriptor #n	m
Reserved	255-m

GFF_ID (011F)

Accept FC-4 Feature,011F Frame				
Word	Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4-35	FC-4 Features (128bytes)			

GID_ID (0121)

Accept Port Identifiers,0121 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Reserved	Port Identifiers		

GIPP_ID (012B)

Accept IP Address (Port) ,012B Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT.)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Request/Response Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4-7	IP Address (Port)			

GID_PT (01A1)

Accept Port Identifiers, 01A1 Frame				
Word	**Bits 31-24**	**Bits 23-16**	**Bits 15-8**	**Bits 7-0**
0	FC_CT Rev =01	IN_ID (S to zero by the Requesting_CT)		
1	GS_TYPE	GS_Subtype	Options	Reserved
2	Command Code		Maximum/Residual Size	
3	Reserved	Reason Code	Reason Code Explanation	Vendor Unique
4	Control rrrr	Port Identifier #1		
	Control #n	Port Identifier #n		

Fibre Channel Protocol Information

The Fibre Channel Protocol Information refers to the following:

- "Well-Known Ordered Sets" on page 502
- "Port State Machine Values" on page 505
- "Well-Known Addresses" on page 506
- "Valid AL_PA Addresses" on page 507

Well-Known Ordered Sets

An ordered set is a transmission word that uses 8B/10B mapping and begins with the K28.5 character. Ordered sets occur outside of frames, and include the following items:

- Primitive signals: Indicate events.
- Frame delimiters: Mark frame boundaries and describe frame contents.
- Primitive sequences: Indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

Types of Ordered Sets

There are two types of Ordered Sets:

- Point-to-Point Link. See "Point to Point Link - Primitive Signals" on page 502 and "Point to Point Link - Primitive Sequences" on page 503.
- Arbitrated Loop. See "Arbitrated Loop - Primitive Signals" on page 504 and "Arbitrated Loop - Primitive Sequences" on page 505.

Point to Point Link - Primitive Signals

The point to point link primitive signals in Table 127 indicate switch events.

Table 127: Point-to-Point Link - Primitive Signals

Abbreviation	Primitive Signal	Ordered Set
Idle	Idle	K28.5 - D21.4 - D21.5 - D21.5
R_RDY	Receiver_Ready	K28.5 - D21.4 - D10.2 - D10.2
VC_RDY	Virtual Circuit Ready	K28.5 - D21.7 - VC_ID - VC_ID
BB_SCs	buffer-to-buffer State Change (SOF)	K28.5 - D21.4 – D22.4 – D22.4
BB_SCr	buffer-to-buffer State Change (R_RDY)	K28.5 - D21.4 – D22.6 – D22.6
SYNx	Clock Synchronization Word X	K28.5 – D31.3 – CS_X – CS_X
SYNy	Clock Synchronization Word Y	K28.5 – D31.3 – CS_Y – CS_Y
SYNz	Clock Synchronization Word Z	K28.5 – D31.3 – CS_Z – CS_Z

Point to Point Link - Primitive Sequences

The point to point link primitive signals in Table 128 indicate port states.

Table 128: Point-to-Point Link - Primitive Sequences

Primitive Sequence	Definition	Ordered Set
Not_Operational (NOS)	■ Loss-of-Synchronization for more than a timeout period (R_T_TOV) while in the Word Synchronization Acquired State ■ Loss-of-Signal while in the Word Synchronization Acquired State ■ Timeout (R_T_TOV) during the Link Reset Protocol	K28.5 D21.2 D31.5 D5.2

Table 128: Point-to-Point Link - Primitive Sequences (Continued)

Primitive Sequence	Definition	Ordered Set
Offline (OLS)	The FC_Port transmitting the Sequence is: ■ initiating the Link Initialization Protocol ■ receiving and recognizing NOS *and* ■ entering the Offline State	K28.5 D21.1 D10.4 D21.2
Link_Reset (LR)	Transmitted by an FC_Port to initiate the Link Reset Protocol, or to recover from a Link Timeout.	K28.5 D9.2 D31.5 D9.2
Link_Reset_Response (LRR)	Transmitted by an FC_Port to indicate that it is receiving and recognizes the LR Primitive Sequence.	K28.5 D21.1 D31.5 D9.2

Table 129 shows the arbitrated loop primitive signals.

Table 129: Arbitrated Loop - Primitive Signals

Abbreviation	Primitive Signal	Ordered Set
ARByx	Arbitrate	K28.5 D20.4 y x
ARB(val)	Arbitrate	K28.5 D20.4 val val
CLS	Close	K28.5 D5.4 D21.5 D21.5
DHD	Dynamic Half-Duplex	K28.5 D10.4 D21.5 D21.5
MRKtx	Mark	K28.5 D31.2 MK_TP AL_PS
OPNyx	Open full-duplex	K28.5 D17.4 AL_PD AL_PS
OPNyy	Open half-duplex	K28.5 D17.4 AL_PD AL_PD
OPNyr	Open selective replicate	K28.5 D17.4 AL_PD D31.7
OPNfr	Open broadcast replicate	K28.5 D17.4 D31.7 D31.7

Table 130 shows the arbitrated loop primitive sequences.

Table 130: Arbitrated Loop - Primitive Sequences

Abbreviation	Primitive Sequence	Ordered Set
LIP(F7,F7)	Loop Initialization–F7, F7	K28.5 D21.0 D23.7 D23.7
LIP(F8,F7)	Loop Initialization–F8, F7	K28.5 D21.0 D24.7 D23.7
LIP(F7,x)	Loop Initialization–F7, x	K28.5 D21.0 D23.7 AL_PS
LIPyx	Loop Initialization–reset	K28.5 D21.0 AL_PD AL_PS
LIPfx	Loop Initialization–reset all	K28.5 D21.0 D31.7 AL_PS
LIPba	Loop Initialization–reserved	K28.5 D21.0 b a
LPByx	Loop Port Bypass	K28.5 D9.0 AL_PD AL_PS
LPBfx	Loop Port Bypass all	K28.5 D9.0 D31.7 AL_PS
LPEyx	Loop Port Enable	K28.5 D5.0 AL_PD AL_PS
LPEfx	Loop Port Enable all	K28.5 D5.0 D31.7 AL_PS

Table 131 shows the port state machine (pstate) values.

Table 131: Port State Machine Values

Port	Value	Description
0	AC	Active state
	IDLE	Idle
1	LR1	Link Reset: LR transmit state
	LR2	Link Reset: LR receive state
	LR3	Link Reset: LRR receive state
	LF1	Link Failure: NOS transmit state
	LF2	Link Failure: NOS receive state
3	OL1	Offline: OLS transmit state

Well-Known Addresses

In the Fibre Channel protocol, a Well-Known Address is a logical address defined by the Fibre Channel standards as assigned to a specific function, and stored on the switch. Table 132 describes the Well-Known Addresses.

Table 132: Well-Known Addresses

Well-Known Address	Description
0xFFFFFF	BROADCAST - Frames transmitted to this address are broadcast to all operational N_Ports.
0xFFFFFE	FABRIC_F_PORT- A Fabric is required to support this address to accept Fabric login (FLOGI) requests from an F_Port, or FL_Port associated with an N_Port or group of NL_Ports on an arbitrated loop.
0xFFFFFD	FABRIC_CONTROLLER - This address is responsible for managing the Fabric. It initializes the Fabric, and routes frames to the Well-Known Address.
0xFFFFFC	NAME_SERVER - This address provides a registration service allowing an N_Port to register information in a database or initiate database queries to retrieve information about other ports.
0xFFFFFB	TIME_SERVER - an optional service that facilitates the maintenance of system time between ports.
0xFFFFFA	MANAGEMENT_SERVER - an optional service used to collect and report management information such as link usage, error statistics, and link quality.
0xFFFFF9	Quality of Service Facilitator (QoSF) for Class-4 Bandwidth and Latency Management (FC_PH2).
0xFFFFF8	ALIAS_SERVER - an optional service to manage the assignment of alias address identifiers.
0xFFFFF7	Security-Key Distribution Service - is an optional service to manage the distribution of encryption security keys to facilitate secure communications between N_Ports.
0xFFFFF6	Clock Synchronization Server (FC-PH3)
0xFFFFF5	MULTICAST SERVER (FC-PH3) - an optional service that manages the reliable multicast function in Class -6. ACK and RJT responses from members of a multicast group, and sending a single reply to the multicast originator.
0xFFFFF4 - 0xFFFFF0	Reserved

Table 132: Well-Known Addresses (Continued)

Well-Known Address	Description
S_ID and D_ID Assignments	
0xFFFBxx	Multicast (group in lower byte)
0xFFFCxx	Embedded_Port (domain in lower byte)

Valid AL_PA Addresses

Arbitrated Loop Physical Address (AL_PA) and Loop IDs are listed in Table 133.

There are 127 possible devices on a loop. AL_PA 00 is the Master AL_PA, which is normally reserved for the FL_Port. The remaining 126 AL_PA values between x01 and xEF are available for use by NL_Ports. The next AL_PAs are EF, E8, E4, and so on from the lowest priority. There are only 127 values on a LOOP because the other bits are used to preserve the running disparity on the link, and AL_PA values are restricted to those characters that result in neutral disparity after encoding.

Table 133: Valid AL_PA Addresses

Word 0		Word 2		Word 3		Word 4	
Bit	AL_PA	Bit	AL_PA	Bit	AL_PA	Bit	AL_PA
31	L_bit	31	3C	31	73	31	B3
30	00	30	43	30	74	30	B4
29	01	29	45	29	75	29	B5
28	02	28	46	28	76	28	B6
27	04	27	47	27	79	27	B9
26	08	26	49	26	7A	26	BA
25	0F	25	4A	25	7C	25	BC
24	10	24	4B	24	80	24	C3
23	17	23	4C	23	81	23	C5
22	18	22	4D	22	82	22	C6
21	1B	21	4E	21	84	21	C7
20	1D	20	51	20	88	20	C9

Table 133: Valid AL_PA Addresses (Continued)

Word 0		Word 2		Word 3		Word 4	
Bit	AL_PA	Bit	AL_PA	Bit	AL_PA	Bit	AL_PA
19	1E	19	52	19	8F	19	CA
18	1F	18	53	18	90	18	CB
17	23	17	54	17	97	17	CC
16	25	16	55	16	98	16	CD
15	26	15	56	15	9B	15	CE
14	27	14	59	14	9D	14	D1
13	29	13	5A	13	9E	13	D2
12	2A	12	5C	12	9F	12	D3
11	2B	11	63	11	A3	11	D4
10	2C	10	65	10	A5	10	D5
9	2D	9	66	9	A6	9	D6
8	2E	8	67	8	A7	8	D9
7	31	7	69	7	A9	7	DA
6	32	6	6A	6	AA	6	DC
5	33	5	6B	5	AB	5	E0
4	34	4	6C	4	AC	4	E1
3	35	3	6D	3	AD	3	E2
2	36	2	6E	2	AE	2	E4
1	39	1	71	1	B1	1	E8
0	3A	0	72	0	B2	0	EF

glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

ABTS
Abort Basic Link Service. Also referred to as “Abort Sequence.”

ACC
Accept link service reply. The normal reply to an Extended Link Service request (such as FLOGI), indicating that the request has been completed.

address identifier
A 24-bit or 8-bit value used to identify the source or destination of a frame. Refer to S_ID and DID.

AL_PA
Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop. Alternately, “arbitrated loop parameters.”

AL_TIME
Arbitrated loop time-out value. Twice the amount of time it would take for a transmission word to propagate around a worst-case loop. The default value is 15 milliseconds (ms).

alias
A logical grouping of elements in a fabric. An alias is a collection of port numbers and connected devices, used to simplify the entry of port numbers and WWNs when creating zones.

alias address identifier
An address identifier recognized by a port in addition to its standard identifier. An alias address identifier can be shared by multiple ports. *See also* alias.

alias AL_PA
An AL_PA value recognized by an L_Port in addition to the AL_PA assigned to the port. *See also* AL_PA.

alias server
A fabric software facility that supports multicast group management.

ARB
Arbitrative primitive signal. Applies only to an arbitrated loop topology. Transmitted as the fill word by an L_Port to indicate that the port is arbitrating access to the loop.

arbitrated loop
A shared 100-MB/sec Fibre Channel transport structured as a loop. Can support up to 126 devices and one fabric attachment. *See also* topology.

arbitration
A method of gaining orderly access to a shared-loop topology.

area number
In Fabric OS v4.0 and above, ports on a switch are assigned a logical area number. Port area numbers can be viewed by issuing the `switchshow` command. They are used to define the operative port for many Fabric OS commands: for example, area numbers can be used to define the ports within an alias or zone.

ARR
Asynchronous response router. Refers to Management Server GS_Subtype Code E4, which appears in `portlogdump` command output.

ASD
Alias server daemon. Used for managing multicast groups by supporting the create, add, remove, and destroy functions.

ASIC
Application-specific integrated circuit. *[Necessary? Basic. –ed.]*

ATM
Asynchronous Transfer Mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity and allows nodes to transmit simultaneously.

authentication
The process of verifying that an entity in a fabric (such as a switch) is what it claims to be. *See also* digital certificate, switch-to-switch authentication.

autocommit
A feature of the `firmwaredownload` command. Enabled by default, `autocommit` commits new firmware to both partitions of a control processor.

autoreboot
Refers to the **-b** option of the `firmwaredownload` command. Enabled by default.

BB_Credit
Buffer-to-buffer credit. The number of frames that can be transmitted to a directly connected recipient or within an arbitrated loop. Determined by the number of receive buffers available. *See also* buffer-to-buffer flow control.

beacon
A tool in which all of the port LEDs on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by a CLI command or through HP Web Tools.

beginning running disparity
The disparity at the transmitter or receiver when the special character associated with an ordered set is encoded or decoded. *See also* disparity.

BIST
Built-in self-test.

bit synchronization
The condition in which a receiver is delivering retimed serial data at the required bit error rate.

block
As it applies to Fibre Channel technology, upper-level application data that is transferred in a single sequence.

bloom
The code name given to the third-generation Fabric ASIC. This ASIC is used in HP StorageWorks 2 GB switches.

broadcast
The transmission of data from a single source to all devices in the fabric, regardless of zoning. *See also* multicast, unicast.

buffer-to-buffer flow control
Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop. *See also* BB_Credit.

bypass circuitry
Circuits that automatically remove a device from the data path when valid signals are dropped.

CA
Certificate authority. A trusted organization that issues digital certificates. *See also* digital certificate.

CAM
Content-addressable memory.

Class 1 service
The class of frame-switching service for a dedicated connection between two communicating ports (also called *connection-oriented service*). Includes acknowledgement of frame delivery or nondelivery.

Class 2 service
A connectionless class of frame-switching service that includes acknowledgement of frame delivery or nondelivery.

Class 3 service
A connectionless class of frame-switching service that does not include acknowledgement of frame delivery or nondelivery. Can be used to provide a multicast connection between the frame originator and recipients, with acknowledgement of frame delivery or nondelivery.

Class 4 service
A connection-oriented service that allows fractional parts of the bandwidth to be used in a virtual circuit.

Class 6 service
A connection-oriented multicast service geared toward video broadcasts between a central server and clients.

Class F service
The class of frame-switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports. Includes acknowledgement of data delivery or nondelivery.

class of service
A specified set of delivery characteristics and attributes for frame delivery.

CLS
Close primitive signal. Used only in an arbitrated loop. Sent by an L_Port that is currently communicating in the loop, to close communication to another L_Port.

configuration

(1) A set of parameters that can be modified to fine-tune the operation of a switch. Use the `configshow` command to view the current configuration of your switch.

(2) In Zoning, a zoning element that contains a set of zones. The Configuration is the highest-level zoning element and is used to enable or disable a set of zones on the fabric. *See also* zone configuration.

COS

Class of service.

CP

Control processor.

credit

As it applies to Fibre Channel technology, the number of receive buffers available to transmit frames between ports. *See also* BB_Credit.

D_ID

Destination identifier. A 3-byte field in the frame header, used to indicate the address identifier of the N_Port to which the frame is headed.

defined zone configuration

The set of all zone objects defined in the fabric. Can include multiple zone configurations. *See also* zone configuration.

digital certificate

An electronic document issued by a CA (certificate authority) to an entity, containing the public key and identity of the entity. Entities in a secure fabric are authenticated based on these certificates. *See also* authentication, CA, public key.

disparity

The proportion of 1s and 0s in an encoded character. *Neutral disparity* means an equal number of each, *positive disparity* means a majority of 1s, and *negative disparity* means a majority of 0s.

DLS

Dynamic load-sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

domain controller

A domain controller (or embedded port) communicates with and gets updates from other switches' embedded ports. The well-known address is fffcdd, where dd = domain number).

domain ID
A unique identifier for all switches in a fabric, used in routing frames. Usually automatically assigned by the principal switch but can be assigned manually. The domain ID for an HP StorageWorks switch can be any integer between 1 and 239.

E_D_TOV
Error-detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error is declared. *See also* R_A_TOV, RR_TOV.

E_Port
Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. *See also* ISL.

ELP
Exchange link parameters.

ELS
Extended link service. ELSs are sent to the destination N_Port to perform the requested function or service. ELS is a Fibre Channel standard that is sometimes referred to as *Fibre Channel Physical (FC_PH) ELS*.

EM
Environmental monitor. Monitors FRUs and reports failures.

embedded port
An embedded port (or domain controller) communicates and get updates from other switches' embedded ports. The well-known address is `fffcdd`, where *dd* = domain number.

entry fabric
The basic HP software license that allows one E_Port per switch.

EOF
End of frame. A group of ordered sets used to mark the end of a frame.

error
As it applies to the Fibre Channel industry, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

exchange
The highest-level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, it can work in either one or both directions.

F_BSY
Fabric port busy frame. A frame issued by the fabric to indicate that a frame cannot be delivered because the fabric or destination N_Port is busy.

F_Port
Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. *See also* FL_Port, Fx_Port.

F_RJT
Fabric port reject frame. A frame issued by the fabric to indicate that delivery of a frame is being denied, perhaps because a class is not supported, there is an invalid header, or no N_Port is available.

fabric
A Fibre Channel network containing two or more switches in addition to hosts and devices. Also referred to as a *switched fabric*. *See also* SAN, topology.

Fabric Manager
Fabric Manager is a GUI that allows for fabric-wide administration and management. Switches can be treated as groups, and actions such as firmware downloads can be performed simultaneously.

fabric name
The unique identifier assigned to a fabric and communicated during login and port discovery.

fabric services
Codes that describe the communication to and from any well-known address.

fabric topology
The arrangement of switches that form a fabric.

Fabric Watch
Fabric Watch can be accessed through either the command line or Advanced Web Tools, and it provides the ability to set thresholds for monitoring fabric conditions.

failover
Describes the HP StorageWorks Core Switch 2/64 process of one CP passing active status to another CP. A failover is nondisruptive.

FAN
Fabric address notification. Retains the AL_PA and fabric address when a loop reinitializes, if the switch supports FAN.

FC-0
Lowest layer of Fibre Channel transport. Represents physical media.

FC-1
Layer of Fibre Channel transport that contains the 8b/10b encoding scheme.

FC-2
Layer of Fibre Channel transport that handles framing and protocol, frame format, sequence/exchange management, and ordered set usage.

FC-3
Layer of Fibre Channel transport that contains common services used by multiple N_Ports in a node.

FC-4
Layer of Fibre Channel transport that handles standards and profiles for mapping upper-level protocols such as SCSI and IP onto the Fibre Channel Protocol.

FC-CT
Fibre Channel common transport.

FC-FG
Fibre Channel generic requirements.

FC-GS
Fibre Channel generic services.

FC-GS-2
Fibre Channel generic services, second generation.

FC-GS-3
Fibre Channel Generic Services, third generation.

FC_IP
Fibre Channel-Over-IP.

FC-PH
The Fibre Channel physical and signaling standard for FC-0, FC-1, and FC-2 layers of the Fibre Channel Protocol. Indicates signaling used for cable plants, media types, and transmission speeds.

FCP
Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FCS
See Fibre Channel.

FCS switch
Relates to the Secure Fabric OS feature. One or more designated switches that store and manage security parameters and configuration data for all switches in the fabric. They also act as a set of backup switches to the primary FCS switch. *See also* primary FCS switch.

FC-SW-2
The second-generation Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches to create a multiswitch Fibre Channel fabric.

FDMI
Fabric-Device Management Interface. FDMI is a database service provided by the fabric for Nx_Ports. The primary use is by HBA devices that register information about themselves and their ports.

FFFFF5
Well-known Fibre Channel address for a Class 6 multicast server.

FFFFF6
Well-known Fibre Channel address for a clock synchronization server.

FFFFF7
Well-known Fibre Channel address for a security key distribution server.

FFFFF8
Well-known Fibre Channel address for an alias server.

FFFFF9
Well-known Fibre Channel address for a QoS facilitator.

FFFFFA
Well-known Fibre Channel address for a management server.

FFFFFB
Well-known Fibre Channel address for a time server.

FFFFFC
Well-known Fibre Channel address for a directory server.

FFFFFD
Well-known Fibre Channel address for a fabric controller.

FFFFFE
Well-known Fibre Channel address for a fabric F_Port.

FFFFFF
Well-known Fibre Channel address for a broadcast alias ID.

Fibre Channel
Fibre Channel is a protocol used to transmit data between servers, switches, and storage devices. It is a high-speed, serial, bidirectional, topology-independent, multiprotocol, and highly scalable interconnection between computers, peripherals, and networks.

FIFO
First in, first out. Refers to a data buffer that follows the first in, first out rule.

firmware
The basic operating system provided with the hardware.

FL_Port
Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. *See also* F_Port, Fx_Port.

flash
Programmable nonvolatile RAM (NVRAM) memory that maintains its contents without power.

FLOGI
Fabric login. The process by which an N_Port determines whether a fabric is present and, if so, exchanges service parameters with it. *See also* PLOGI.

frame
The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, optional headers, data payload, cyclic redundancy check (CRC), and end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements and so forth) and data frames.

FRU
Field-replaceable unit. A component that can be replaced onsite.

FSPF
Fabric shortest path first. The routing protocol for Fibre Channel switches.

FSS
Fabric OS state synchronization. The FSS service is related to high availability (HA). The primary function of FSS is to deliver state update messages from active components to their peer standby components. FSS determines if fabric elements are synchronized (and thus FSS compliant).

FTP
File Transfer Protocol.

full fabric
The software license that allows multiple E_Ports on a switch, making it possible to create multiple ISL links.

full fabric citizenship
A loop device that has an entry in the Simple Name Server.

full-duplex
A mode of communication that allows the same port to simultaneously transmit and receive frames. *See also* half-duplex.

Fx_Port
A fabric port that can operate as either an F_Port or FL_Port. *See also* F_Port, FL_Port.

G_Port
Generic port. A port that can operate as either an E_Port or an F_Port. A port is defined as a G_Port when it is not yet connected or has not yet assumed a specific function in the fabric.

gateway
Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC
Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical-level transport for Fibre Channel and gigabit Ethernet.

Gb/sec
Gigabits per second (1,062,500,000 bits/second).

GB/sec
Gigabytes per second (1,062,500,000 bytes/second).

GLM
Gigabit Link Module. A semitransparent transceiver that incorporates serializing and deserializing functions.

GMT
Greenwich Mean Time. An international time zone. Also known as *UTC*.

GUI
A graphic user interface, such as Web Tools and Fabric Manager.

HA
High availability. A set of features in HP StorageWorks switches that is designed to provide maximum reliability and nondisruptive replacement of key hardware and software modules.

half-duplex
A mode of communication that allows a port to either transmit or receive frames at any time except simultaneously (with the exception of link control frames, which can be transmitted at any time). *See also* full-duplex.

hard address
The AL_PA that an NL_Port attempts to acquire during loop initialization.

HBA
Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

header
A Fibre Channel frame has a header and a payload. The header contains control and addressing information associated with the frame.

HiPPI
High-Performance Parallel Interface. An 800 Mb/sec interface normally used in supercomputer environments.

hop count
The number of ISLs a frame must traverse to get from its source to its destination.

host
A computer system that provides end users with services like computation and storage access.

HTTP
Hypertext Transfer Protocol. The standard TCP/IP transfer protocol used on the World Wide Web.

hub
A Fibre Channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

I2C
Related to internal circuitry on motherboard. *[Is this useful?]*

idle
Continuous transmission of an ordered set over a Fibre Channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.

in-band
Transmission of management protocol over the Fibre Channel.

initiator
A server or workstation on a Fibre Channel network that initiates communications with storage devices. *See also* target.

Insistent Domain ID Mode
Sets the domain ID of a switch as insistent, so that it remains the same over reboots, power cycles, failovers, and fabric reconfigurations.

interswitch link
See ISL.

IOCTL
I/O control.

IP
Internet Protocol. The addressing part of TCP.

ISL
Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. *See also* E_Port.

isolated E_Port
An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). *See also* E_Port.

IU
Information unit. A set of information as defined by either an upper-level process protocol definition or upper-level protocol mapping.

JBOD
Just a bunch of disks. Indicates a number of disks connected in a single chassis to one or more controllers. *See also* RAID.

K28.5
A special 10-bit character used to indicate the beginning of a transmission word that performs Fibre Channel control and signaling functions. The first seven bits of the character are the comma pattern.

key
A string of data (usually a numeric value) shared between two entities and used to control a cryptographic algorithm. Usually selected from a large pool of possible keys to make unauthorized identification of the key difficult. *See also* key pair.

key pair
In public key cryptography, a pair of keys consisting of an entity's public and private key. The public key can be publicized, but the private key must be kept secret. *See also* public key cryptography.

L_Port
Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in either Fabric Mode or Loop Mode.

LAN
Local area network. A network in which transmissions typically take place over fewer than 5 kilometers (3.4 miles).

latency
The time required to transmit a frame. Together, latency and bandwidth define the speed and capacity of a link or system.

LED
Light-emitting diode. Used to indicate the status of elements on a switch.

LIFA
Loop-initialization fabric-assigned frame. Contains a bitmap of all fabric-assigned AL_PAs and is the first frame transmitted in the loop initialization process after a temporary loop master has been selected.

LIHA
Loop-initialization hard-assigned frame. A hard-assigned AL_PA that is indicated by a bit set and is the third frame transmitted in the loop initialization process after a temporary loop master has been selected.

LILP
Loop-initialization loop-position frame. The final frame transmitted in a loop initialization process. A returned LIRP contains an accumulation of all of the AL_PA position maps. This allows loop members to determine their relative loop position. This is an optional frame and is not transmitted unless the LIRP is also transmitted.

Link Services
A protocol for link-related actions.

LIP
Loop initialization primitive. The signal used to begin initialization in a loop. Indicates either loop failure or node resetting.

LIPA
Loop-initialization previously assigned. The device marks a bit in the bitmap if it did not log in with the fabric in a previous loop initialization.

LIRP
Loop-initialization report position frame. The first frame transmitted in the loop initialization process after all L_Ports have selected an AL_PA. The LIRP gets transmitted around the loop so all L_Ports can report their relative physical position. This is an optional frame.

LISA
Loop-initialization soft-assigned frame. The fourth frame transmitted in the loop initialization process after a temporary loop master has been selected. L_Ports that have not selected an AL_PA in a LIFA, LIPA, or LIHA frame select their AL_PA here.

LISM
Loop-initialization select master frame. The first frame transmitted in the initialization process when L_Ports select an AL_PA. LISM is used to select a temporary loop master or the L_Port that subsequently starts transmission of the LIFA, LIPA, LIHA, LISA, LIRP, or LILP frames.

LM_TOV
Loop master timeout value. The minimum time that the loop master waits for a loop initialization sequence to return.

loop initialization
The logical procedure used by an L_Port to discover its environment. Can be used to assign AL_PA addresses, detect loop failure, or reset a node.

looplet
A set of devices connected in a loop to a port that is a member of another loop.

LR
Link reset. A primitive sequence used during link initialization between two N_Ports in point-to-point topology or an N_Port and an F_Port in fabric topology. The expected response is an LRR.

LRR
Link reset response. A primitive sequence during link initialization between two N_Ports in point-to-point topology or an N_Port and an F_Port in fabric topology. It is sent in response to an LR and expects a response of Idle.

MALLOC
Memory allocation. Usually relates to buffer credits.

MB/sec
Megabytes per second.

Mb/sec
Megabits per second.

metric
A relative value assigned to a route to aid in calculating the shortest path (1000 at 1 Gb/sec, 500 at 2 Gb/sec).

MIB
Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

MRK
Mark primitive signal. Used only in arbitrated loop, MRK is transmitted by an L_Port for synchronization and is vendor specific.

MS
Management Server. The Management Server allows a storage area network (SAN) management application to retrieve information and administer the fabric and interconnected elements, such as switches, servers, and storage devices. The MS is located at the Fibre Channel well-known address fffffah.

multicast
The transmission of data from a single source to multiple specified N_Ports (as opposed to all the ports on the network). *See also* broadcast, <Italic>unicast.

N_Port
Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. *See also* NL_Port, Nx_Port.

Name Server
Simple Name Server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also referred to as *directory service*.

NL_Port
Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. *See also* N_Port, Nx_Port.

node

A Fibre Channel device that contains an N_Port or NL_Port.

node count
The number of nodes attached to a fabric.

node name
The unique identifier for a node, communicated during login and port discovery.

NOS
Not operational. The NOS primitive sequence is transmitted to indicate that the FC_Port transmitting the NOS has detected a link failure or is offline, waiting for the offline sequence (OLS) to be received.

NS
Name Server. The service provided by a fabric switch that stores names, addresses, and attributes related to Fibre Channel objects. Can cache information for up to 15 minutes. Also known as *Simple Name Server* or as a *directory service*. *See also* SNS.

Nx_Port
A node port that can operate as either an N_Port or NL_Port.

OLS
Primitive sequence offline.

ON
Offline notification. Refers to an ELS field that appears in `portlogdump` command output.

OPN
Open primitive signal. Applies only to arbitrated loop; sent by an L_Port that has won the arbitration process to open communication with one or more ports on the loop.

ordered set
A transmission word that uses 8B/10B mapping and begins with the K28.5 character. Ordered sets occur outside of frames and include the following items:

Frame delimiters. Mark frame boundaries and describe frame contents.

Primitive signals. Indicate events.

Primitive sequences. Indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage frame transport.

originator
The Nx_Port that originated an exchange.

out-of-band
Transmission of management protocol outside of the Fibre Channel network, usually over Ethernet.

OX_ID
Originator ID. Refers to the exchange ID assigned by the originator port.

parallel
The simultaneous transmission of data bits over multiple lines.

path selection
The selection of a transmission path through the fabric. HP StorageWorks switches use the FSPF protocol. *See also* FSPF.

payload
A Fibre Channel frame has a header and a payload. The payload contains the information being transported by the frame; it is determined by the higher-level service or FC_4 upper-level protocol. There are many different payload formats, based on protocol and size of truck bed.

Performance Monitoring
An HP StorageWorks switch feature that monitors port traffic and includes frame counters, SCSI read monitors, SCSI write monitors, and other types of monitors.

persistent error log
Error messages of a high enough level (by default, Panic or Critical) are saved to flash memory on the switch instead of to RAM. These messages are saved over reboots and power cycles, constituting the persistent error log. Note that each CP on a Core Switch 2/64 has its own unique persistent error log.

phantom address
An AL_PA value that is assigned to a device that is not physically in the loop. Also known as *phantom AL_PA*.

phantom device
A device that is not physically in an arbitrated loop but is logically included through the use of a phantom address.

PID
Port identifier.

PKI
Public key infrastructure. An infrastructure that is based on public key cryptography and CA (certificate authority) and that uses digital certificates. *See also* CA, digital certificate, public key cryptography.

PKI certification utility
Public key infrastructure certification utility. A utility that makes it possible to collect certificate requests from switches and to load certificates to switches. *See also* digital certificate, PKI.

PLOGI
Port login. The port-to-port login process by which initiators establish sessions with targets. *See also* FLOGI.

point-to-point
A Fibre Channel topology that employs direct links between each pair of communicating entities. *See also* topology.

port
In an HP StorageWorks switch environment, an SFP or GBIC receptacle on a switch to which an optic cable for another device is attached.

port address
In Fibre Channel technology, the port address is defined in hexadecimal. In the Fabric OS, a port address can be defined by a domain and port number combination or by area number. In an ESCON Director, an address used to specify port connectivity parameters and to assign link addresses for attached channels and control units.

port card
A hardware component that provides a platform for field-replaceable, hot-swappable ports.

port log
A record of all activity on a switch, kept in volatile memory.

port log dump
A view of what happens on a switch, from the switch's point of view. The `portlogdump` command is used to read the port log.

port name
A user-defined alphanumeric name for a port.

port swapping
Port swapping is the ability to redirect a failed port to another port. This feature is available in Fabric OS v4.1.0 and later.

port_name
The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

POST
Power-on self-test. A series of tests run by a switch after it is turned on.

primary FCS switch
Relates to the Secure Fabric OS feature. The primary fabric configuration server switch actively manages security and configurations for all switches in the fabric.

primitive sequence
An ordered set that is transmitted repeatedly and continuously. Primitive sequences are transmitted to indicate specific conditions within or conditions encountered by the receiver logic of an FC_Port. *See* OLS *and* NOS.

primitive signals
An ordered set that indicates actions or events and requires just one occurrence to trigger a response. Idle and R_RDY are used in all three topologies: ARB, OPN, and CLS. MRK is used in arbitrated loop.

principal switch
The first switch to boot up in a fabric. Ensures unique domain IDs among roles.

private key
The secret half of a key pair. *See also* key, key pair.

private loop
An arbitrated loop that does not include a participating FL_Port.

private loop device
A device that supports a loop and can understand 8-bit addresses but does not log in to the fabric.

private NL_Port
An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to the fabric.

protocol
A defined method and set of standards for communication. Determines the type of error-checking, the data-compression method, how sending devices indicate an end of message, and how receiving devices indicate receipt of a message.

pstate
Port State Machine.

public device
A device that supports arbitrated loop protocol, can interpret 8-bit addresses, and can log in to the fabric.

public key
The public half of a key pair. *See also* key, key pair.

public key cryptography
A type of cryptography that uses a key pair, with the two keys in the pair called at different points in the algorithm. The sender uses the recipient's public key to encrypt the message, and the recipient uses the recipient's private key to decrypt it. *See also* key pair, PKI.

public loop
An arbitrated loop that includes a participating FL_Port and can contain both public and private NL_Ports.

public NL_Port
An NL_Port that logs in to the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

QoS
Quality of service.

quad
A group of four adjacent ports that share a common pool of frame buffers.

queue
A mechanism for each AL_PA address that allows for collecting frames prior to sending them to the loop.

R_A_TOV
Resource allocation timeout value. The maximum time a frame can be delayed in the fabric and still be delivered. *See also* E_D_TOV, RR_TOV.

R_CTL
Route control. The first 8 bits of the header, which defines the type of frame and its contents.

R_RDY
Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

R_T_TOV
Receiver transmitter timeout value, used by receiver logic to detect loss of synchronization between transmitters and receivers.

RAID
Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. *See also* JBOD.

RCS
Reliable Commit Service. Refers to the ILS command code.

remote switch
An optional product for long-distance fabrics, requiring a Fibre Channel-to-ATM or SONET gateway.

responder
The N_Port with which an exchange originator wishes to communicate.

RLS
Read Link Status.

route
As it applies to a fabric, the communication path between two switches. Might also apply to the specific path taken by an individual frame, from source to destination. *See also* FSPF.

routing
The assignment of frames to specific switch ports, according to frame destination.

RR_TOV
Resource recovery timeout value. The minimum time a target device in a loop waits after a LIP before logging out an SCSI initiator. *See also* E_D_TOV, R_A_TOV.

RSCN
Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes. The fabric controller issues RSCN requests to N_Ports and NL_Ports, but only if they have registered to be notified of state changes in other N_Ports and NL_Ports. This registration is performed via the State Change Registration (SCR) Extended Link Service. An N_Port or NL_Port can issue an RSCN to the fabric controller without having completed SCR with the fabric controller.

RTWR
Reliable transport with response. Might appear as a task in `portlogdump` command output.

running disparity
A binary parameter indicating the cumulative disparity (positive or negative) of all previously issued transmission characters.

RW
Read/write. Refers to access rights.

RX
Receiving frames.

RX_ID
Responder exchange identifier. A 2-byte field in the frame header that can be used by the responder of the exchange to identify frames as being part of a particular exchange.

S_ID
Source ID. Refers to the native port address (24 bit address).

SAN
Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. *See also* fabric.

SAN architecture
The overall design of a storage network solution, which includes one or more related fabrics, each of which has a topology.

SAN port count
The number of ports available for connection by nodes in the entire SAN.

SCN
State change notification. Used for internal state change notifications, not external changes. This is the switch logging that the port is online or is an Fx_port, not what is sent from the switch to the Nx_ports.

SCR
State change registration. Extended Link Service (ELS) requests the fabric controller to add the N_Port or NL_Port to the list of N_Ports and NL_Ports registered to receive the Registered State Change Notification (RSCN) Extended Link Service.

SCSI
Small Computer Systems Interface. A parallel bus architecture and a protocol for transmitting large data blocks to a distance of 15 to 25 meters.

sectelnet
A protocol similar to Telnet but with encrypted passwords for increased security.

Secure Fabric OS
A separately sold feature that provides advanced, centralized security for a fabric.

security policy
Rules that determine how security is implemented in a fabric. Security policies can be customized through Secure Fabric OS or Fabric Manager.

SEQ_ID
Sequence identifier. A 1-byte field in the frame header change to identify the frames as being part of a particular exchange sequence between a pair of ports.

sequence
A group of related frames transmitted in the same direction between two N_Ports.

sequence initiator
The N_Port that begins a new sequence and transmits frames to another N_Port.

sequence recipient
Serializing/deserializing circuitry. A circuit that converts a serial bit stream into parallel characters, and vice-versa.

SES
SCSI Enclosure Services. A subset of the SCSI protocol used to monitor temperature, power, and fan status for enclosed devices.

SFP
Small-form-factor pluggable. A transceiver used on 2 GB/sec switches that replaces the GBIC.

Simple Name Server (SNS)
A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also referred to as *directory service* or *name server.*

Single CP Mode
The **-s** option of the `firmwaredownload` command. Using `firmwaredownload -s` enables Single CP Mode. In the Core Switch 2/64, Single CP Mode enables a user to upgrade a single CP and to select full-install, auto-reboot, and auto-commit.

SNMP
Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols.

SNS
Simple Name Server.

SOF
Start of frame. A group of ordered sets that marks the beginning of a frame and indicates the class of service the frame uses.

SONET
Synchronous optical network. A standard for optical networks that provides building blocks and flexible payload mappings.

special character
A 10-bit character that does not have a corresponding 8-bit value but is still considered valid. The special character is used to indicate that a particular transmission word is an ordered set. This is the only type of character to have five 1s or 0s in a row.

SSH
Secure shell. Used starting in Fabric OS v4.1 to support encrypted Telnet sessions to the switch. SSH encrypts all messages, including the client sending the password at login.

switch
A fabric device providing bandwidth and high-speed routing of data via link-level addressing.

switch name
The arbitrary name assigned to a switch.

switch port
A port on a switch. Switch ports can be E_Ports, F_Ports, or FL_Ports.

switch-to-switch authentication
The process of authenticating both switches in a switch-to-switch connection using digital certificates. *See also* authentication, digital certificate.

syslog
Syslog daemon. Used to forward error messages.

T11
A standards committee chartered with creating standards for Fibre Channel.

target
A storage device on a Fibre Channel network. *See also* initiator.

TC
Track changes.

Telnet
A virtual terminal emulation used with TCP/IP. Telnet is sometimes used as a synonym for the Fabric OS CLI.

tenancy
The time from when a port wins arbitration in a loop until the same port returns to the monitoring state. Also referred to as *loop tenancy*.

Time Server
A Fibre Channel service that allows for the management of all timers.

topology
As it applies to Fibre Channel technology, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

Point to point. A direct link between two communication ports.

Switched fabric. Multiple N_Ports linked to a switch by F_Ports.

Arbitrated loop. Multiple NL_Ports connected in a loop.

track changes
A Fabric OS feature that can be enabled to report specific activities (for example, logins, logouts, and configuration task changes). The output from the track-changes feature is dumped to the error log for the switch.

transceiver
A device that converts one form of signaling to another for transmission and reception; in fiber optics, optical to electrical.

Translative Mode
A mode in which private devices can communicate with public devices across the fabric.

transmission character
A 10-bit character encoded according to the rules of the 8B/10B algorithm.

transmission word
A group of four transmission characters.

trap (SNMP)
The message sent by an SNMP agent to inform the SNMP management station of a critical error. *See also* SNMP.

trunking
In Fibre Channel technology, a feature that enables distribution of traffic over the combined bandwidth of up to four ISLs between adjacent switches, while preserving in-order delivery.

trunking group
A set of up to four trunked ISLs.

trunking ports
The ports in a set of trunked ISLs.

TS
Time Server.

TTL
Time-to-live. The number of seconds an entry exists in cache before it expires.

tunneling
A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network but are connected by a different type of network.

TX
Transmit.

U_Port
Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or FL_Port. A port is defined as a U_Port when it is not connected or has not yet assumed a specific function in the fabric. *[How is this different from a G_Port?]*

unicast
The transmission of data from a single source to a single destination. *See also* broadcast, multicast.

UTC
Universal Time Conversion. Also known as *Coordinated Universal Time*, which is an international standard of time. UTC is eight hours ahead of Pacific Standard Time and five hours ahead Eastern Standard Time. See also GMT.

WAN
Wide area network.

watchdog
A software daemon that monitors Fabric OS modules on the kernel.

well-known address
As it pertains to Fibre Channel technology, a logical address defined by Fibre Channel standards as assigned to a specific function and stored on the switch.

WWN
World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

zone
A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access to others in the zone but are not visible to any outside the zone.

zone configuration
A specified set of zones. Enabling a configuration enables all zones in that configuration. *See also* defined zone configuration.

zoning
A feature in fabric switches or hubs that allows segmentation of a node by physical port, name, or address.

index

L

M

N

P

S